

## Guides pratiques

Chaque Guide pratique explique comment utiliser un gratuiciel ou un logiciel de source ouverte (Open Source). On y présente les difficultés potentielles, on y donne des conseils pratiques et, surtout, on vous montre comment configurer et utiliser ces outils de façon sûre. Chaque guide comporte plusieurs captures d'écran, ainsi qu'un mode d'emploi point par point pour vous aider à suivre la démarche.

Tous ces logiciels peuvent être installés directement à partir du Guide pratique ou téléchargés gratuitement du site du développeur. Dans la plupart des cas, il vous sera possible d'installer un outil simplement en cliquant sur le lien approprié situé au début du guide associé à cet outil, puis en indiquant à votre navigateur d'Ouvrir ou d'Installer le programme. Si un Guide pratique fournit des instructions d'installation particulières, il vous faudra peut-être sauvegarder un fichier sur votre Bureau ou à un autre emplacement avant d'installer cet outil.

Pour des raisons de sécurité, vous devriez toujours utiliser la plus récente version des programmes présentés ici. La version de certains des programmes présentés ici est peut-être plus récente que celle utilisée lors de la rédaction du guide pratique correspondant. Dans ce cas, l'interface de la nouvelle version peut différer légèrement de celle décrite dans ce guide, mais pas substantiellement.

Les guides pratiques proposent également, si le cas se présente, des versions « portables » de quelques outils importants de la trousse Security in-a-box. Ces versions sont conçues pour être extraites directement vers une clé de mémoire USB pour que vous puissiez ensuite les utiliser à partir de n'importe quel ordinateur. Dans la mesure où les outils portatifs ne sont pas installés sur un ordinateur local, leur existence et leur utilisation peuvent passer inaperçues. Cependant, gardez à l'esprit que votre périphérique externe ou clé de mémoire USB ainsi que tout outil portable ne sont aussi sûrs que votre ordinateur et courent également le risque d'être exposés à des logiciels publicitaires, malveillants ou espions et à des virus.

## Avast - antivirus

### Short Description:

**avast!** est un programme antivirus complet qui sert à détecter et éliminer les virus et logiciels malveillants de votre ordinateur. Bien qu'**avast!** soit gratuit pour utilisation non commerciale sur un ordinateur familial ou personnel, votre copie gratuite *doit* être enregistrée après l'installation, à défaut de quoi elle expirera après 30 jours. L'enregistrement vous assurera également de recevoir automatiquement les mises à jour du programme **Avast!**, ainsi que les plus récentes définitions de virus au fur et à mesure de leur publication.

### Online Installation Instructions:

#### Pour installer avast!

- Lisez la courte **Introduction aux Guides pratiques** <sup>[1]</sup>
- Cliquez sur l'icône **avast!** ci-dessous pour ouvrir la page de téléchargement d'[www.avast.com](http://www.avast.com).
- Cliquez sur le bouton 'Télécharger' au bas de la colonne 'Antivirus Gratuit', puis cliquez sur le lien 'Télécharger' qui s'affiche sur la prochaine page.
- Cliquez sur 'Enregistrer le fichier' pour sauvegarder le fichier 'setup\_av\_free\_fre.exe' sur votre ordinateur, puis **double-cliquez** sur 'setup\_av\_free\_fre.exe' pour lancer l'installation du programme.
- Lisez attentivement la section **2.0 Comment installer et enregistrer avast!** avant de poursuivre.
- Après avoir complété l'installation d'**avast!** vous pouvez supprimer l'exécutable d'installation de votre ordinateur.

avast!:



Site Internet:

[www.avast.com](http://www.avast.com) <sup>[3]</sup>

Configuration requise:

- Compatible avec toutes les versions de Windows

Version utilisée pour rédiger ce guide:

- 5.0

Licence:

- Gratuiciel

Lecture préalable:

- Livret pratique Security-in-a-Box, chapitre **1. Protéger votre ordinateur contre les logiciels malveillants et les pirates** <sup>[4]</sup>

Niveau: 1: Débutant, 2: Moyen, 3: Intermédiaire, 4: Expérimenté, 5: Avancé

Temps d'apprentissage: 20 minutes

## Ce que vous apportera l'utilisation de cet outil:

- La capacité de scanner votre ordinateur pour y détecter des virus et les éliminer.
- La capacité de protéger votre ordinateur contre les nouveaux virus et toute nouvelle infection.
- La capacité de recevoir des mises à jour des définitions de virus depuis Internet.

## Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

Bien que nous recommandions l'**antivirus gratuit d'avast!** dans ce chapitre, il existe d'autres programmes compatibles avec **Microsoft Windows** qui valent également la peine qu'on s'y intéresse:

- **Avira AntiVir Personal Edition** <sup>[5]</sup> et
- **AVG Anti-Virus** <sup>[6]</sup>.

Par ailleurs, si vous avez les moyens d'acheter la version commerciale du programme antivirus pour **Microsoft Windows**, vous en retirerez probablement une protection plus complète.

Bien que les systèmes d'exploitation comme **GNU Linux** et **Mac OS** soient pratiquement épargnés des virus, il existe plusieurs bonnes raisons pour y installer des programmes contre les virus et les programmes malveillants. D'abord, des virus seront éventuellement créés pour ces systèmes d'exploitation, et deuxièmement, vous courez le risque de répandre des virus à votre insu, même si votre propre système est protégé.

À l'heure actuelle, il n'existe malheureusement aucun programme antivirus *gratuit* que nous serions à l'aise de recommander pour **Linux** et **Mac OS**. Cependant, il existe plusieurs produits *commerciaux* qui présentent de nombreux avantages et une excellente protection. Voici la liste des programmes les plus populaires:

- **avast!** <sup>[7]</sup>,
- **Kaspersky** <sup>[8]</sup>,
- **Mcafee** <sup>[9]</sup>,
- **Sophos** <sup>[10]</sup>, et
- **Symantec** <sup>[11]</sup>, entre autres.

Si vous pouvez vous permettre d'acheter une copie de l'un ou l'autre de ces programmes, n'hésitez pas à le faire.

## 1.1 À propos de cet outil

Les virus informatiques sont des programmes malveillants qui peuvent détruire des fichiers, ralentir votre ordinateur et utiliser votre carnet d'adresses pour trouver et infecter d'autres ordinateurs. Avast est un programme antivirus complet qui protège votre ordinateur contre les virus qui pourraient y accéder par téléchargement depuis Internet, par courriel (pièce jointe) ou par transfert depuis un support amovible (CD, DVD, disquette, clé USB, etc.).

- Assurez-vous de ne pas avoir deux programmes antivirus installés et actifs simultanément. Si vous utilisez présentement un autre programme et souhaitez changer pour **avast!**, vous devez d'abord désinstaller l'autre programme antivirus avant d'installer **avast!**.
- De nouveaux virus sont conçus à tous les jours. Pour protéger efficacement votre ordinateur, **avast!** doit être en mesure de mettre à jour régulièrement votre base de données virale.
- Les virus les plus insidieux sont ceux qui empêchent carrément l'installation de **avast!** et ceux qu'**avast!** n'est pas en mesure de détecter et supprimer. Dans une situation comme celle-là, il vous faudra recourir à des méthodes un peu plus avancées, dont certaines sont abordées à la section **4.9 Méthodes avancées de suppression des virus** <sup>[12]</sup>.

### Offline Installation Instructions :

#### Pour installer Avast!

- \*Lisez la courte **Introduction** aux **Guides pratiques** <sup>[1]</sup>\*\*
- **Cliquez sur l'icône Avast! ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.

Avast!:



## Comment installer et enregistrer avast!


Sommaire des sections de cette page:

- **2.0 Comment installer avast!**
- **2.1 Comment enregistrer avast!**

---

### 2.0 Comment installer avast!

L'installation de **avast!** est relativement simple et rapide. Pour commencer, suivez les étapes énumérées ci-dessous:

**Première étape.** Double-cliquez sur  `setup_av_free_fre` ; si une fenêtre *Fichier ouvert - Avertissement de sécurité* s'affiche, cliquez sur  pour activer la barre de progression du décompactage, qui peut prendre jusqu'à une minute, selon la vitesse de votre ordinateur. Lorsque toutes les composantes de **avast!** seront décompactées, la boîte de dialogue suivante s'affichera (NDT: Si vous installez le programme à partir du fichier d'installation français, l'assistant passe directement à la deuxième étape décrite ci-dessous.)

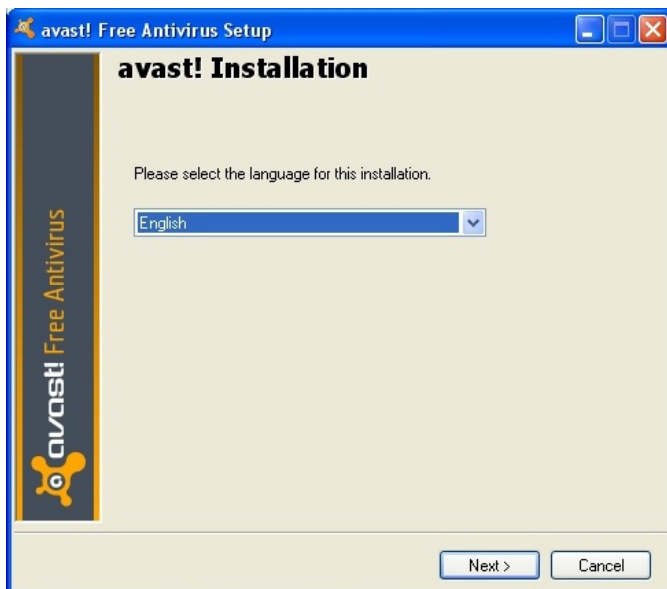


Figure 1: La fenêtre d'installation d'avast! Free Antivirus

Deuxième étape. Cliquez sur  pour afficher la fenêtre suivante:

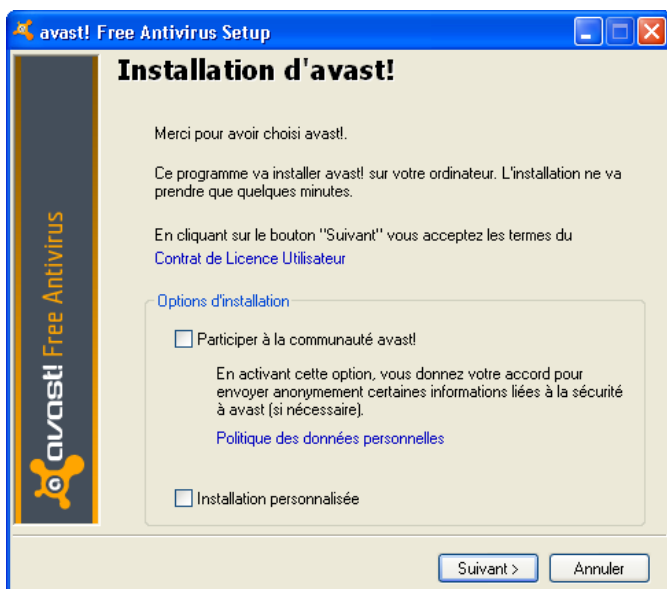


Figure 2: La fenêtre d'installation d'avast!

Lors du processus d'installation d'avast!, la fenêtre d'installation s'affiche avec l'option *Participer à la communauté avast!* automatiquement sélectionnée. Pour des raisons de sécurité et de confidentialité, il est préférable que vous désactiviez cette option, tel qu'illustré à la Figure 2, ci-dessus.

Troisième étape. Décochez la case *Participer à la communauté avast!* pour désélectionner cette option, puis cliquez sur  pour afficher la prochaine fenêtre:

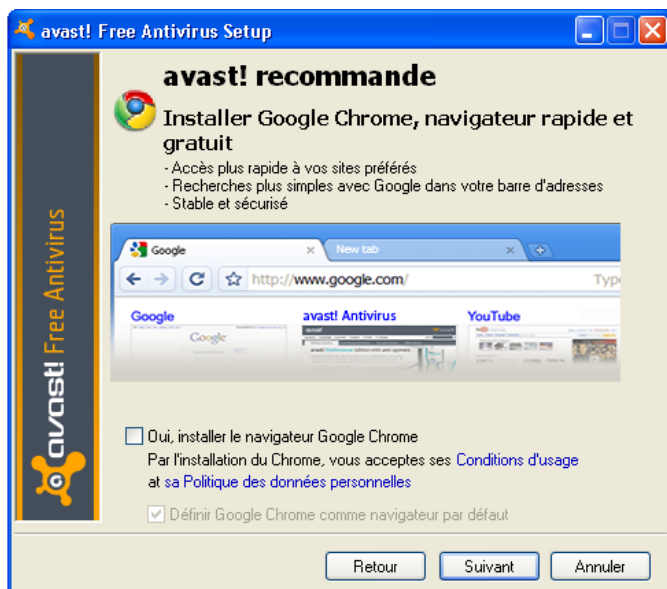


Figure 3: La fenêtre avast! recommande

Lors du processus d'installation d'**avast!**, la fenêtre *avast! recommande* s'affiche avec l'option *Oui, installer le navigateur Google Chrome* automatiquement sélectionnée. Il est préférable de désactiver cette option, tel qu'illustré à la figure 3, ci-dessus.

**Quatrième étape. Décochez** la case *Oui, installer le navigateur Google Chrome* pour désélectionner cette option, puis cliquez sur  pour poursuivre l'installation d'**avast!**.

Un message s'affichera après quelques minutes pour vous indiquer que le processus d'installation est terminé.

**Cinquième étape. Cliquez** sur  pour finaliser le processus d'installation du logiciel. Quelques secondes plus tard, un icône **avast!** apparaît dans votre *Barre d'état système*:



Figure 4: L'icône avast! surlignée en noir dans Barre d'état système

Quelques secondes plus tard, un autre message s'affiche pour confirmer l'installation d'**avast!**:



Figure 5: Le message de confirmation de l'installation d'avast!

Chaque fois qu'**avast!** opère une mise à jour automatique du programme ou de la base de données virale, un message s'affiche au dessus de la *Barre d'état système*, tel qu'illustré ci-dessous:



Figure 6: Un exemple de message d'avast!

**Important:** Vous devez enregistrer votre copie du programme pour vous assurer que la base de données virale et le logiciel lui-même soient régulièrement mis à jour automatiquement.

Lorsque vous aurez correctement enregistré votre copie d'**avast!**, le programme protégera automatiquement votre ordinateur contre les virus et les logiciels malveillants. En cas d'attaque, **avast!** affichera des messages d'avertissement comme celui-ci:



Figure 7: Un exemple d'avertissement indiquant qu'une menace a été bloquée.


**Sixième étape.** Double-cliquez sur  dans la Barre d'état système (voir la figure 4) pour ouvrir la fenêtre principale d'avast!, puis cliquez sur [Plus de détails...](#) pour afficher les détails de l'État actuel, tel qu'illustré ci-dessous:



Figure 8: La fenêtre principale du programme avast!

**Important:** Vous devez enregistrer **avast!** pour continuer à recevoir les mises à jour du programme et des définitions de virus, qui sont essentielles à la protection de votre ordinateur contre diverses menaces.

## 2.1 Comment enregistrer avast!

**Commentaire:** Si vous n'enregistrez pas votre copie d'**avast!**, celle-ci cessera de fonctionner après 30 jours. Il vous faut être connecté à Internet pour enregistrer **avast!**.

Pour enregistrer votre copie d'**avast!**, suivez les étapes énumérées ci-dessous:

**Première étape.** Cliquez sur  pour afficher la fenêtre principale d'avast! (Figure 10).

**Deuxième étape.** Cliquez sur [Enregistrez-vous maintenant](#) (par les menus MAINTENANCE et Enregistrement) pour afficher les deux fenêtres suivantes successivement:

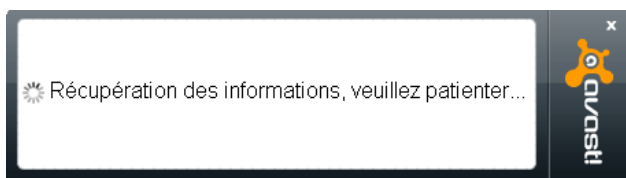


Figure 9: Fenêtre d'enregistrement d'avast! antivirus gratuit

La fenêtre d'Enregistrement d'avast! antivirus gratuit vous informe que des informations sont en cours de récupération. Une deuxième fenêtre vous avise que votre copie d'**avast!** expirera dans 30 jours si vous ne l'enregistrez pas d'ici là. (La même fenêtre affiche également des renseignements sur les versions commerciales du logiciel et les promotions en cours.)



Figure 10: La fenêtre d'état de votre enregistrement

Troisième étape. Cliquez sur **S'enregistrer** pour afficher à nouveau la boîte illustrée à la figure 2, suivie immédiatement de cette fenêtre:

Figure 11: Le formulaire d'enregistrement d'avast! antivirus gratuit

**Commentaire:** Les seuls champs *obligatoires* sont le *Nom* et l'*E-mail*. Ils sont identifiés par des astérisques et encadrés d'une ligne pointillée rouge. Les autres champs sont facultatifs.

Quatrième étape. Saisissez votre nom et votre adresse de courriel dans les champs appropriés, puis cliquez sur

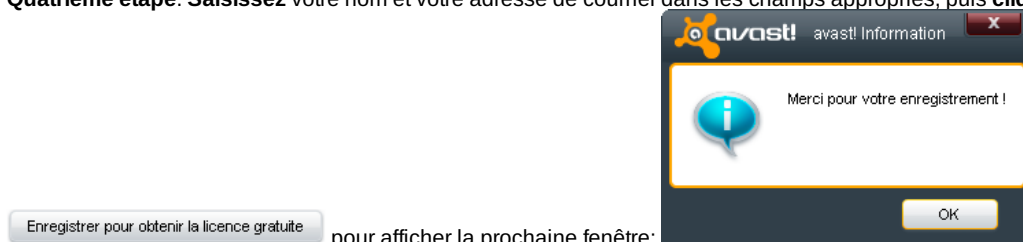


Figure 12: Fenêtre pop-up Merci pour votre enregistrement

Cinquième étape. Cliquez sur **OK** pour afficher le panneau *VOTRE ENREGISTREMENT* dans la fenêtre

principale du programme:



Figure 13: Le panneau VOTRE ENREGISTREMENT qui confirme l'enregistrement de votre copie d'avast!

Vous avez complété l'enregistrement de votre copie d'**avast!** et êtes maintenant en position d'apprendre comment mettre manuellement à jour le programme et les définitions de virus. Pour ce faire, veuillez lire la section **3.0 Comment mettre à jour avast! manuellement**.

## Comment mettre à jour avast! manuellement

Sommaire des sections de cette page :


- **3.0 Avant de commencer**
- **3.1 Comment lancer une mise à jour par l'interface principale d'avast!**
- **3.2 Comment lancer une mise à jour par le menu local d'avast!**
- **3.3 Comment désactiver la fonction de mise à jour automatique d'avast!**

---

### 3.0 Avant de commencer

**avast!** marche discrètement en arrière-plan de votre ordinateur et exécute automatiquement des mises à jour du programme et des définitions de virus chaque fois que vous vous connectez à Internet. Cela dit, si votre accès à Internet est temporaire ou sporadique, il sera peut-être plus pratique ou efficace de lancer les mises à jour manuellement lorsque cela vous convient.

**Commentaire:** Il existe deux méthodes pour lancer les mises à jour d'**avast!** manuellement. Vous pouvez lancer une mise à jour à partir de l'interface principale d'**avast!** ou en passant par le menu local qui se déploie lorsque vous cliquez à droite sur l'icône **avast!** de la *Barre d'état système*. De plus, il est possible de désactiver l'option de mise à jour automatique

dans la fenêtre *RÉGLAGES PRINCIPAUX*, en cliquant sur  dans le coin supérieur droit de l'interface principale.

#### Comment lancer une mise à jour par l'interface principale d'avast!

Pour mettre à jour **avast!** manuellement à partir de l'interface principale, suivez les étapes énumérées ci-dessous:

**Première étape.** Cliquez sur  pour afficher l'interface principale d'**avast!**, illustrée ci-dessous:



Figure 1: L'onglet Résumé affichant le panneau État actuel, où figure un avis typique de mise à jour de la Version du programme

Une mise à jour du programme ou des définitions de virus est indiquée par un icône orange marqué d'un point d'exclamation, au lieu de l'icône vert marqué d'un crochet. La mise à jour du programme ou de la définition de virus est affichée en rouge et un bouton *Mise à jour* est désormais visible.

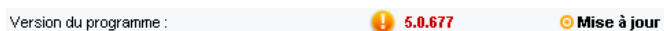


Figure 2: Une nouvelle version du programme est disponible

**Deuxième étape:** Cliquez sur **Mise à jour** pour lancer la mise à jour. À l'issue de la mise à jour, la sous-fenêtre *Version du programme* s'affiche comme ceci:

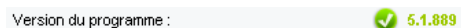


Figure 3: La Version du programme est mise à jour

Le programme est passé de la version 5.0.677 à la version 5.1.889.

La liste ci-dessous décrit brièvement chacun des items ou icônes d'état du panneau *État actuel SÉCURISÉ*:

**Astuce:** Cliquez sur **Plus de détails...** pour afficher ou cacher les renseignements du panneau *État actuel*

**Protection résidente:** Cet icône indique si la protection résidente fonctionne normalement. La protection résidente surveille l'activité de votre ordinateur; il y a des protections résidentes dédiées au courriel, au système de fichier local, à l'activité sur Internet, ainsi qu'à d'autres systèmes. Lorsqu'une protection résidente est désactivée, que ce soit volontairement ou sous l'effet d'un programme malveillant, l'icône d'**avast!** dans la *Barre d'état système* change d'apparence pour refléter ce changement d'état:

**Mise à jour automatique de la VPS:** Cet icône indique si le mécanisme de mise à jour automatique est activé ou non.

**Version de la base de données virale VPS:** Cet icône indique la date de publication de la plus récente définition de virus. La date est affichée de la façon suivante: 11 réfère à l'année 2011, 01 réfère au mois et 17 réfère au jour.

**Version du programme:** Cet icône indique la plus récente mise à jour de la version du programme.

**Date d'expiration:** Cet item indique la date et l'heure d'expiration de votre copie d'**avast!**; vous devez renouveler ou ré-enregistrer votre copie avant cette date.



**Troisième étape.** Cliquez sur **MAINTENANCE** pour afficher la fenêtre ci-dessous:





Figure 4: L'interface principale affichant le panneau MAINTENANCE MISE À JOUR

Le panneau MAINTENANCE MISE À JOUR peut être utilisé pour mettre à jour manuellement le programme et les définitions de virus.

**Quatrième étape:** Cliquez sur pour lancer la mise à jour du moteur et des définitions de virus.

**Cinquième étape:** Cliquez sur quand la mise à jour est complétée pour retourner au panneau MAINTENANCE MISE À JOUR.

Le processus est le même pour mettre à jour le programme **avast!**.

**Sixième étape:** Cliquez sur pour lancer la mise à jour du programme.

**Septième étape:** Cliquez sur quand la mise à jour est complétée pour retourner au panneau MAINTENANCE MISE À JOUR.

### 3.2 Comment lancer une mise à jour par le menu local d'avast!

Les mises à jour du programme et des définitions de virus d'**avast!** peuvent être exécutées à partir du menu local **avast!**. Il est possible d'accéder directement au panneau MAINTENANCE MISE À JOUR d'**avast!** par le menu local qui se trouve dans la *Barre d'état système*.

Pour lancer manuellement les mises à jour du *moteur et de la base de données virale* à partir du menu local, suivez les étapes énumérées ci-dessous:

**Première étape:** Cliquez à droite sur dans la *barre d'état système* pour afficher le menu local illustré ci-dessous:

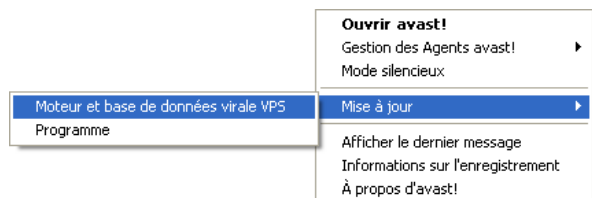


Figure 5: Le menu local d'avast!


**Deuxième étape:** Sélectionnez Mise à jour > Moteur et base de données virale VPS pour afficher la Figure 4, puis suivez les étapes 4 et 5.

**Troisième étape:** Sélectionnez Mise à jour > Programme pour afficher la Figure 6, puis suivez les étapes 6 et 7 décrite à la section 3.1 Comment lancer une mise à jour par l'interface principale d'avast!

### 3.3 Comment désactiver la fonction de mise à jour automatique d'avast!

En mode par défaut, **avast!** est configuré pour télécharger automatiquement les mises à jour du programme et de la base de données virale. Vous pouvez cependant désactiver cette fonction en cliquant sur le bouton *Paramètres*, qui se trouve

dans le coin supérieur droit de l'interface principale.

**Première étape.** Cliquez sur  pour activer la fenêtre *RÉGLAGES PRINCIPAUX* d'**avast!**, puis sélectionnez *Mises à jour* pour afficher le panneau *RÉGLAGES DES MISES À JOUR*.

**Deuxième étape.** Cliquez sur l'option *Mise à jour manuelle* dans les rubriques *MOTEUR ET BASE DE DONNÉES VIRALE VPS* et *PROGRAMME*.

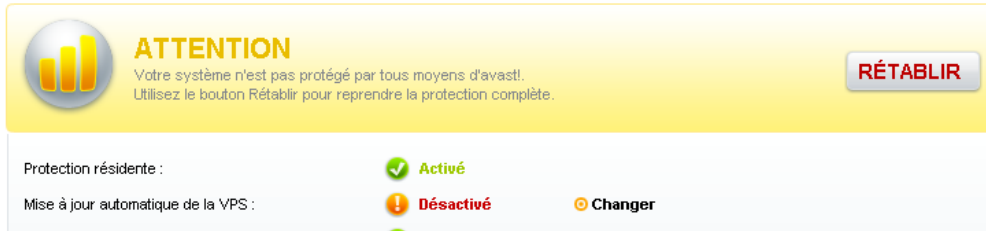



Figure 6: Le panneau *RÉSUMÉ ATTENTION* indiquant que la *Mise à jour automatique de la VPS* est désactivée

Les utilisateurs avancés voudront peut-être raffiner davantage leurs réglages dans les rubriques *Détails* et *Réglage du Proxy*. Pour ce faire, suivez les étapes énumérées ci-dessous:

**Troisième étape.** Cliquez sur  pour développer les rubriques *Détails* et *Réglage du Proxy* et en modifier les paramètres.

Vous avez appris les différentes méthodes pour mettre à jour manuellement *le moteur et la base de données virale* et *le programme d'avast!*. Pour commencer à utiliser **avast!**, veuillez lire attentivement la section **4.0 Comment utiliser avast! pour détecter et éliminer des virus**

## Comment utiliser avast! pour détecter et éliminer des virus

Sommaire des sections de cette page:

- [4.0 Avant de commencer](#)
- [4.1 Comment faire face efficacement à une attaque de virus](#)
- [4.2 Un survol de l'interface principale d'avast!](#)
- [4.3 Comment balayer votre ordinateur pour détecter des programmes malveillants et des virus](#)
- [4.4 Comment exécuter un Scan minutieux du système](#)
- [4.5 Comment exécuter un Scan de dossiers](#)
- [4.6 Comment exécuter un Scan au démarrage](#)
- [4.7 Comment gérer les virus détectés](#)
- [4.8 Comment utiliser la Zone de quarantaine](#)
- [4.9 Méthodes avancées de suppression de virus](#)

---

### 4.0 Avant de commencer

Le traitement efficace des virus et logiciels malveillants à l'aide d'**avast!** comporte deux étapes importantes. Il vous faut d'abord balayer (ou scanner) votre ordinateur pour détecter les menaces. Il faut ensuite éliminer les menaces ou les déplacer vers la *Zone de quarantaine* d'**avast!**. La suppression et/ou le déplacement des virus et logiciels malveillants empêche ceux-ci d'interagir avec d'autres systèmes, tel que le système de fichiers ou les programmes de gestion du courrier électronique.

Il peut paraître étrange de sauvegarder de tels virus ou logiciels malveillants. Mais si ceux-ci se sont attachés à des données importantes ou sensibles, vous voudrez peut-être ultérieurement récupérer ou sauvegarder ces documents, fichiers ou programmes infectés. Dans de rares cas, **avast!** peut se tromper en identifiant des codes et programmes légitimes comme malveillants. Généralement appelés *faux positifs*, ces codes ou programmes sont potentiellement important pour le bon fonctionnement de votre système, il vous faudra peut-être les récupérer ultérieurement.

La *Zone de quarantaine* d'**avast!** est un espace virtuel où vous pouvez examiner un virus et déterminer s'il constitue une authentique menace, soit en effectuant une recherche sur Internet, soit en le soumettant à l'attention d'un laboratoire spécialisé (une option qui s'offre à vous dans **avast!** en cliquant à droite sur un virus listé dans la *Zone de quarantaine*). Cette opération *n'activera pas* le virus ou le logiciel malveillant en question car la *Zone de quarantaine* l'isole du reste de votre système.

**Astuce:** À l'inverse, la *Zone de quarantaine* d'**avast!** peut être utilisée pour y transférer des données importantes ou sensibles et les mettre à l'abri en cas d'attaque de virus.

Dans cette section:

- Nous étudierons les pratiques exemplaires pour protéger votre réseau et/ou votre ordinateur personnel;
- Nous explorerons l'interface principale, et en particulier les onglets LANCER UN SCAN et MAINTENANCE;
- Nous verrons comment exécuter les divers types de scans; et
- Nous verrons comment utiliser la *Zone de quarantaine* d'**avast!**.

### 4.1 Comment faire face efficacement à une attaque de virus

Il y a un ensemble de précautions élémentaires que vous pouvez prendre pour limiter les menaces contre votre ordinateur; par exemple, en évitant les sites douteux ou problématiques ou en utilisant régulièrement des logiciels anti-mouchard et

antivirus comme **avast!** et **Spybot**. Cela dit, il est possible que notre système personnel fasse partie d'un réseau local (LAN) et/ou que l'on partage une connexion Internet. Les considérations qui suivent concernent les façons de réagir efficacement à une attaque de virus lorsque plusieurs ordinateurs sont en réseau, que ce soit en contexte communautaire ou au travail.

- Déconnectez physiquement votre ordinateur d'Internet et du réseau local. Si vous utilisez une connexion sans fil, déconnectez votre ordinateur du réseau sans fil. Si possible, éteignez la machine et retirez la carte de communications sans fil.
- Si votre ordinateur fait partie d'un réseau, vous devriez immédiatement déconnecter tous les ordinateurs d'Internet et du réseau lui-même. Chaque utilisateur devrait cesser d'utiliser le réseau et lancer **avast!** ou un autre programme antivirus fiable afin de détecter et éliminer le virus. Cela peut sembler laborieux, mais cette procédure est essentielle à la protection des ordinateurs personnels et du réseau.
- Planifiez un Scan au prochain démarrage pour chaque ordinateur du réseau. Notez bien le nom de chaque virus détecté, de sorte que vous puissiez effectuer une recherche, puis supprimez-les ou déplacez-les vers la *Zone de quarantaine d'avast!*. Pour vous familiariser avec cette procédure, veuillez consulter la section **4.6 Comment exécuter un Scan au démarrage**.
- Même si un virus a été détecté ou réparé, répétez les étapes précédentes et lancez un scan au démarrage sur chaque ordinateur, jusqu'à ce qu'**avast!** n'affiche plus aucun message d'avertissement. Selon la gravité de l'attaque, il est possible qu'un seul scan au démarrage suffise.

Pour plus de renseignements sur les moyens de défense contre les virus et les logiciels malveillants, veuillez consulter la section **4.9 Méthodes avancées de suppression de virus**

## 4.2 Un survol de l'interface principale d'avast!

L'interface utilisateur d'**avast!** comporte quatre onglets principaux, situés à la gauche de la fenêtre: RÉSUMÉ, LANCER UN SCAN, PROTECTION RÉSIDENTE et MAINTENANCE. Chaque onglet est divisé en sous-onglets qui permettent d'afficher les panneaux correspondants.

**Première étape.** Cliquez sur  pour afficher la fenêtre ci-dessous:



Figure 1: L'onglet RÉSUMÉ affichant le panneau État actuel SÉCURISÉ

La liste ci-dessous détaille brièvement les fonctions des quatre onglets principaux:

**RÉSUMÉ:** Cet onglet comprend les sous-onglets *État actuel* et *Statistiques*. Le sous-onglet *État actuel* affiche l'état des composantes principales utilisées par **avast!** pour défendre votre ordinateur contre les virus et autres attaques. Le panneau *Statistiques* affiche les opérations des composantes de **avast!**. Affichage par semaine, mois ou année.

**LANCER UN SCAN:** Cet onglet comporte les sous-onglets *Scanner maintenant*, *Scan au démarrage* et *Rapports de scans*. Le panneau *SCANNER MAINTENANT* affiche les différentes options de scan manuels. Le panneau *SCAN AU DÉMARRAGE* vous permet de planifier un scan au prochain démarrage de votre ordinateur. Le panneau *RAPPORTS DE SCANS* affiche un rapport des scans manuels effectués, sous forme de tableau.

**PROTECTION RÉSIDENTE:** Cet onglet affiche tous les agents de protection associés aux fonctions de votre ordinateur, dont l'*AGENT DES FICHIERS*. Vous avez ici un accès direct aux réglages des agents de protection, y compris les boutons pour les arrêter et les démarrer.

**MAINTENANCE:** Cet onglet comporte les sous-onglets *Mise à jour*, *Enregistrement*, *Zone de quarantaine* et *À propos d'avast!*. Le panneau *MISE À JOUR* vous permet de lancer manuellement des mises à jour du programme et des définitions de virus. Le panneau *ENREGISTREMENT* vous permet d'enregistrer votre copie d'**avast!**. Le panneau *ZONE DE QUARANTAINE* affiche les virus et logiciels malveillants détectés par **avast!** lors des scans et vous permet de les gérer de différentes façons, soit en les supprimant, en lançant de nouveaux scans ou en soumettant les virus détectés à

l'analyse de laboratoires spécialisés. Le panneau À PROPOS D'AVAST affiche des renseignements sur la plus récente version d'**avast!** installée sur votre ordinateur.

**Commentaire:** Les panneaux *LANCER UN SCAN* et *MAINTENANCE* sont particulièrement pratiques pour traiter les menaces posées par des virus et des logiciels malveillants.

### 4.3 Comment balayer votre ordinateur pour détecter des programmes malveillants et des virus

Dans cette section, nous examinerons les différentes options de scan disponibles, ainsi que leur mode d'emploi. Nous verrons également comment lancer un scan du système, un scan de dossiers et un scan au démarrage.

Le panneau *LANCER UN SCAN* > *SCANNER MAINTENANT* présente les quatre options de scan offertes par **avast!**; pour les afficher, suivez les étapes décrites ci-dessous:



Première étape. Cliquez sur pour afficher la fenêtre suivante:



Figure 2: L'onglet *LANCER UN SCAN* affichant le panneau *SCANNER MAINTENANT*

Les descriptions suivantes vous aideront à choisir le mode de scan le plus approprié:

**Scan rapide:** Cette option est recommandée aux utilisateurs qui ont peu de temps pour détecter de potentielles menaces.

**Scan minutieux:** Cette option est recommandée aux utilisateurs qui ont assez de temps pour lancer un scan minutieux de leur système. Ce mode est également recommandé si vous utilisez le programme antivirus pour la première fois sur votre ordinateur. La durée de ce scan dépend du nombre de documents, de fichiers, de dossiers et de disques durs sur votre ordinateur, ainsi que la vitesse de la machine. Veuillez consulter la section **4.4 Comment exécuter un Scan minutieux du système**.

**Scan des médias amovibles:** Cette option est recommandée pour scanner des disques durs externes, des clés USB et d'autres dispositifs ou supports amovibles, en particulier ceux qui ne vous appartiennent pas. **avast!** tentera de détecter des programmes malveillants conçus pour s'exécuter lorsque le dispositif est connecté.

**Scan des dossiers sélectionnés:** Cette option est recommandée pour scanner un ou plusieurs dossiers en particulier. Cette option est utile si vous soupçonnez qu'un fichier ou un dossier est infecté. Veuillez consulter la section **4.5 Comment exécuter un Scan de dossiers**.

**Astuce:** Chaque option de scan vous permet de voir les détails du scan, par exemple, les secteurs qui sont actuellement balayés. Cliquez sur pour les afficher. Si vous êtes un utilisateur avancé ou expert, cliquez sur pour raffiner les réglages pour chaque mode de scan.

### 4.4 Comment exécuter un Scan minutieux du système

Pour lancer un scan minutieux du système, suivez les étapes décrites ci-dessous:

Première étape. Cliquez sur dans la rubrique du mode *Scan minutieux* pour afficher la fenêtre suivante:

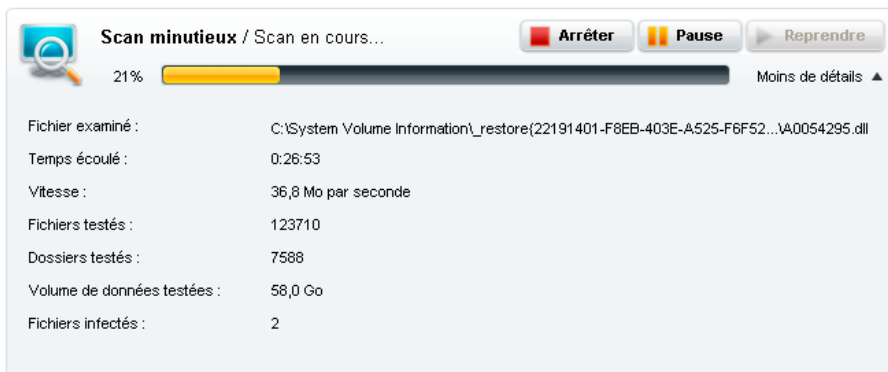


Figure 3: Le panneau SCANNER MAINTENANT affichant le scan minutieux en cours d'exécution

À l'issue du scan minutieux, si une menace a été détectée sur votre ordinateur le panneau *Scan minutieux* ressemblera à ceci:




Figure 4: La rubrique Scan complété affichant un avertissement MENACE DÉTECTÉE!

Le scan minutieux du système a détecté quelques menaces; pour savoir quoi faire à partir de là, veuillez consulter la section [4.7 Comment gérer les virus détectés](#).

La *Zone de quarantaine d'avast!* est un dossier mis en place lors du processus d'installation d'**avast!**; c'est une zone de quarantaine virtuelle où les virus et les logiciels malveillants sont isolés de telle sorte qu'ils ne peuvent pas interagir avec, ou parasiter, les autres processus en cours sur votre ordinateur.

#### 4.5 Comment exécuter un Scan de dossiers

Pour scanner vos dossiers, suivez les étapes décrites ci-dessous:

**Première étape.** Cliquez sur  dans la rubrique du mode *Scan des dossiers sélectionnés* pour afficher la fenêtre suivante:

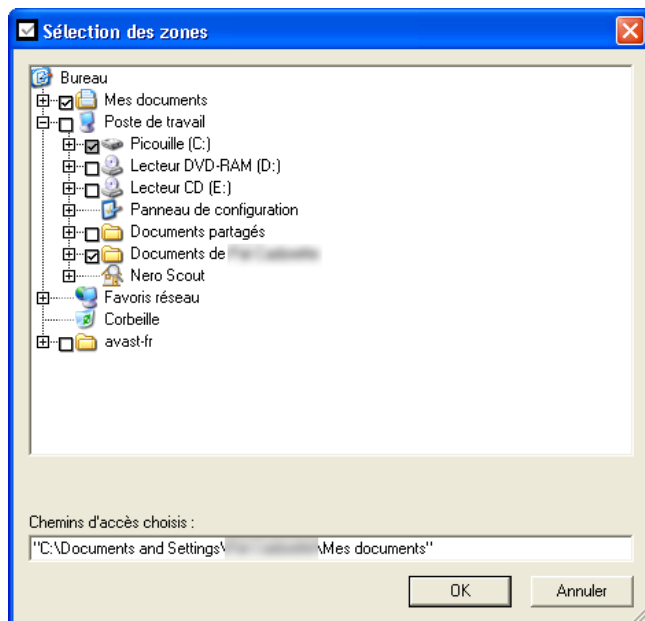


Figure 5: La boîte de dialogue Sélection des zones

La boîte de dialogue *Sélection des zones* vous permet de choisir le dossier que vous souhaitez scanner. Vous pouvez également sélectionner plus d'un dossier. Lorsque vous cochez la case correspondant à chaque dossier, le chemin d'accès du dossier s'affiche dans le champs *Chemins d'accès choisis*:

**Deuxième étape.** Cliquez sur  pour lancer le scan de vos dossiers et afficher la fenêtre suivante:

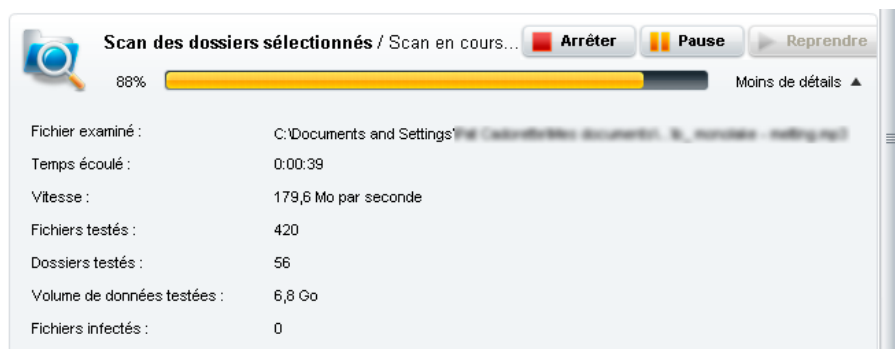



Figure 6: Le Scan de dossiers en cours d'exécution

**Astuce: avast!** vous permet de scanner des dossiers à partir du menu local *Windows* standard qui s'affiche lorsque vous cliquez à droite sur un dossier donné. Vous n'avez qu'à **sélectionner** l'icône  qui apparaît à côté du nom du dossier que vous souhaitez scanner.

#### 4.6 Comment exécuter un Scan au démarrage

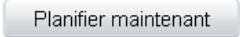
Le scan au démarrage d'**avast!** vous permet de planifier un scan complet de votre disque dur avant que le *Système d'exploitation Windows de Microsoft* ne soit mis en exécution. Au moment où le scan au démarrage s'exécute, la majorité des programmes malveillants sont toujours en dormance, c'est-à-dire, qu'ils n'ont pas encore eu l'occasion de s'activer ou d'interagir avec d'autres processus du système. C'est pourquoi ils sont plus facilement détectables à cette étape.


Le scan au démarrage accède directement au disque sans passer par les pilotes du système de fichier **Windows**, une cible de premier choix pour la plupart des programmes malveillants. Un scan au démarrage devrait être en mesure de détecter même les plus agressifs des "rootkits" (c'est le nom employé pour désigner un type de logiciel malveillant particulièrement pernicieux). Il est **fortement recommandé** de planifier un scan au démarrage si vous avez le moindre soupçon que votre système a été compromis ou infecté.

L'option *Scan au démarrage* est recommandée pour un scan complet et minutieux de votre système. Le scan peut prendre un certain temps, selon la vitesse de votre ordinateur, la quantité de données à examiner et le nombre de disques dur branchés à votre ordinateur. Le *Scan au démarrage* est toujours planifié pour le prochain redémarrage de votre ordinateur.

Pour scanner votre système au prochain démarrage, suivez les étapes décrites ci-dessous:

**Première étape.** Cliquez sur  pour afficher le panneau *SCAN AU DÉMARRAGE*.

**Deuxième étape.** Cliquez sur  pour planifier un scan au prochain démarrage de votre ordinateur.

**Troisième étape.** Cliquez sur  pour lancer le scan au démarrage immédiatement si vous préférez.

**Commentaire:** Un scan au démarrage s'exécute avant que le système d'exploitation et l'interface utilisateur ne soient chargés. C'est pourquoi vous ne verrez qu'un écran bleu affichant le progrès du scan, tel qu'illustré ci-dessous:

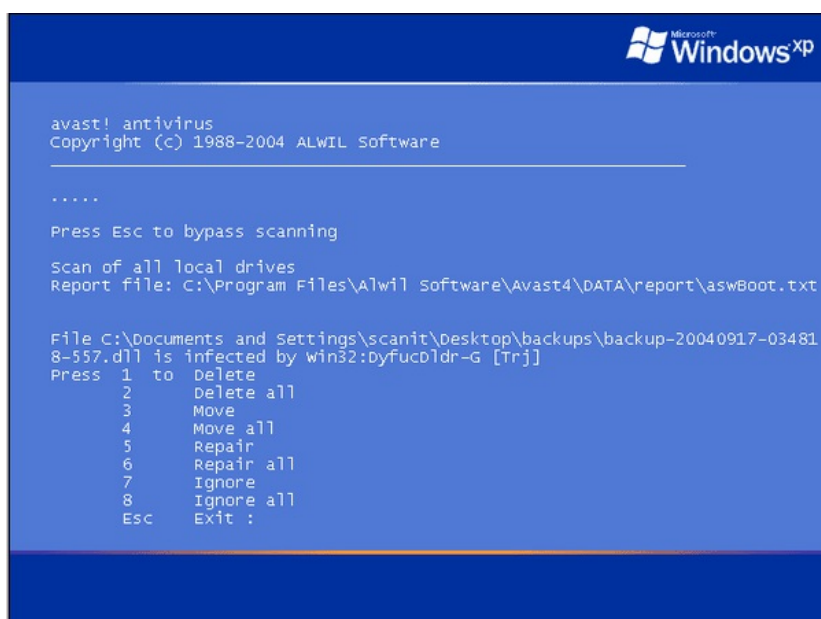


Figure 7: Le scan au démarrage planifié d'**avast!**

Chaque fois qu'**avast!** détecte une menace, le programme vous demande si vous voulez *Supprimer, Ignorer, Mettre en quarantaine* ou *Réparer* les virus détectés. Il est recommandé de ne *jamais* les ignorer. La liste de ces commandes n'apparaît uniquement que si un virus est détecté sur votre système.

#### 4.7 Comment gérer les virus détectés

Lors du processus d'installation d'**avast!**, la *Zone de quarantaine d'avast!* a été créée sur votre disque dur. La *Zone de*

quarantaine n'est ni plus ni moins qu'un dossier qui est isolé du reste de votre système et utilisé pour stocker les logiciels malveillants ou les virus détectés au cours du scan, ainsi que les documents, fichiers et dossiers infectés ou compromis.

Si vous avez déjà mis à jour le programme et la base de données virale, vous êtes déjà familier avec l'onglet **MAINTENANCE**, par lequel vous pouvez également accéder à la *Zone de quarantaine d'avast!*

Pour gérer adéquatement les virus et logiciels malveillants détectés lors du scan, suivez les étapes décrites ci-dessous:

**Première étape.** Cliquez sur **AFFICHER LES RÉSULTATS** pour afficher la fenêtre suivante:

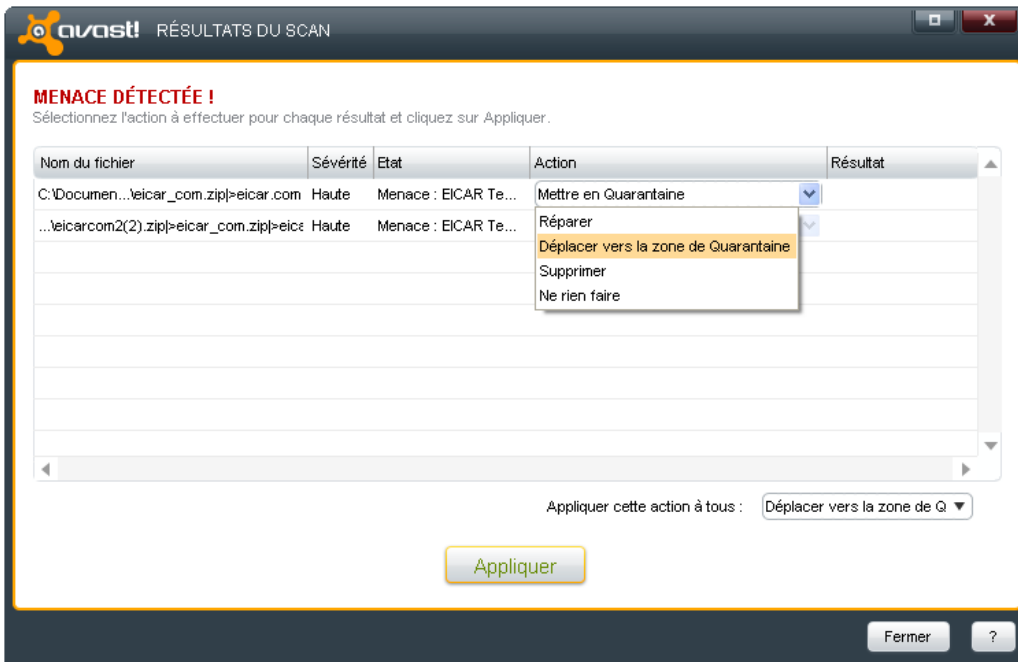


Figure 8: La fenêtre **RÉSULTATS DU SCAN** affichant le message d'avertissement **MENACE DÉTECTÉE!**

**Deuxième étape.** Cliquez sur **Action** pour afficher le menu déroulant présentant la liste des actions qui peuvent être appliquées aux menaces détectées, tel qu'illustré à la *Figure 8*, ci-dessus.

**Commentaire:** Dans cet exercice, nous voulons déplacer les fichiers infectés vers la *Zone de quarantaine*. Cependant, le menu déroulant présente trois autres options que nous décrivons sommairement ci-dessous:

**Réparer:** Cette action tentera de réparer le fichier infecté.

**Supprimer:** Cette action supprimera de façon permanente le fichier infecté.

**Ne rien faire:** Cette action *n'est définitivement pas recommandée* lorsqu'il est question de gérer adéquatement des virus ou des programmes malveillants.


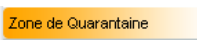
**Troisième étape.** Sélectionnez l'action *Déplacer vers la zone de quarantaine*, puis cliquez sur **Appliquer** pour afficher la fenêtre ci-dessous:



Figure 9: Les virus ont été déplacés vers la Zone de quarantaine

## 4.8 Comment utiliser la Zone de quarantaine

Maintenant que le virus a été déplacé vers la *Zone de quarantaine d'avast!*, vous pouvez déterminer quelle est la meilleure chose à faire.

Première étape. Cliquez sur  puis cliquez sur  pour afficher la fenêtre ci-dessous:

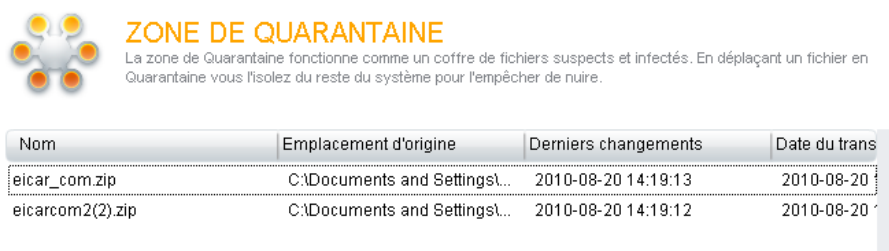


Figure 10: La Zone de quarantaine affichant deux virus

Deuxième étape: Cliquez à droite sur un des virus pour afficher le menu des actions possibles, tel qu'illustré ci-dessous:

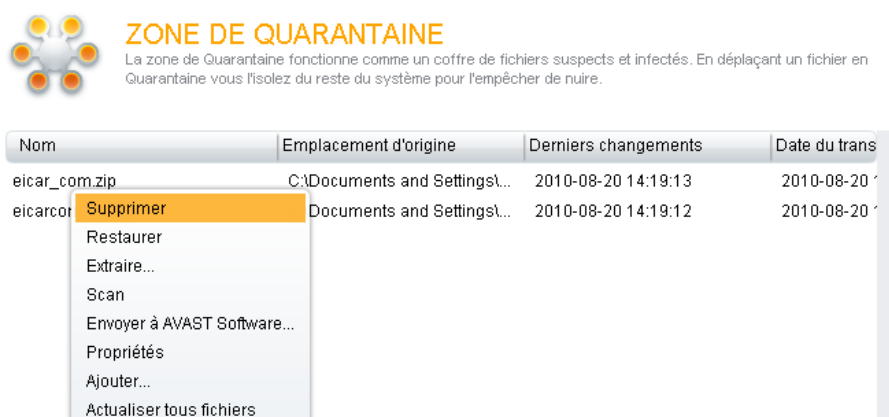


Figure 11: Le menu déroulant des actions à appliquer aux virus dans la Zone de quarantaine

**Commentaire:** Vous n'activerez pas un virus en double-cliquant dessus dans la *Zone de quarantaine*. Cette action affichera plutôt les propriétés du virus, de la même façon que si vous cliquez sur l'option *Propriétés* dans le menu local.

La liste ci-dessous décrit les différentes actions du menu déroulant:

**Supprimer:** Cette action supprimera le virus de façon irréversible.

**Restaurer:** Cette action restaurera les virus à leur emplacement initial.

**Extraire...:** Cette action copiera le fichier ou le virus dans un dossier de votre choix.

**Scan:** Cette action soumettra le virus à un nouveau scan.

**Envoyer à AVAST Software...:** Cette action vous permet de soumettre le virus à une analyse plus poussée. En sélectionnant cette action, vous activerez un formulaire à remplir et à envoyer.

**Propriétés:** Cette action vous permet d'afficher plus de détails concernant le virus en question.

**Ajouter...:** Cette action vous permet de naviguer dans votre système pour chercher d'autres fichiers que vous aimeriez déplacer vers la *Zone de quarantaine*. Cette fonction pourrait s'avérer très utile pour protéger certains fichiers lors d'une attaque de virus.

**Actualiser tous fichiers:** Cette action permet d'opérer une mise à jour des fichiers pour être certain d'afficher les fichiers les plus récents.

## 4.9 Méthodes avancées de suppression de virus

Dans certains cas, la protection fournie par **avast!**, **Comodo Firewall** et **Spybot** n'est tout simplement pas suffisante. Malgré nos efforts les plus rigoureux, nos ordinateurs personnels et de travail sont parfois infectés par des programmes malveillants et des virus. Dans la section **4.1 Comment faire face efficacement à une attaque de virus**, nous avons vu quelques méthodes pour faire face aux virus les plus coriaces. Mais il existe d'autres mesures qui peuvent être mises en place pour éliminer complètement ces menaces.

### Méthode A: Utiliser des CD/DVD de secours anti-logiciel malveillant (Rescue CD)

Certaines des compagnies qui développent des outils contre les programmes malveillants offrent également des CD/DVD de secours, ou Rescue CD/DVD. On peut les télécharger sous forme d'images ISO (un format qui peut être facilement gravé sur un disque CD ou DVD).



Pour utiliser un CD ou un DVD anti-programme malveillant, veuillez suivre les étapes décrites ci-dessous:

1. Téléchargez et gravez le programme anti-logiciel malveillant sur un CD. *Vous pouvez utiliser un logiciel gratuit comme [ImgBurn](#) [14] pour graver l'image sur un disque.*
2. Insérez le disque dans le lecteur de CD/DVD de l'ordinateur infecté, puis redémarrez l'ordinateur à partir du CD/DVD. *Habituellement, vous pouvez démarrer à partir d'un disque en appuyant sur la touche F10 ou F12 du clavier immédiatement après avoir allumé l'ordinateur. Soyez très attentif aux consignes qui s'affichent sur l'écran lors du démarrage pour connaître la méthode appropriée sur votre ordinateur.*
3. Connectez votre ordinateur à Internet pour permettre au programme anti-logiciel malveillant de mettre à jour ses définitions de virus, si nécessaire. Le programme se mettra automatiquement à la recherche des menaces sur votre ordinateur, puis il les supprimera au fur et à mesure.

Voici une liste d'images de CD de secours:

- [AVG Rescue CD](#) [15]
- [Kaspersky Rescue CD](#) [16]
- [F-Secure Rescue CD](#) [17]
- [BitDefender Rescue CD](#) [18]

Il peut aussi être utile de scanner votre ordinateur à l'aide des outils suivants, qui se mettent en marche au démarrage de **Windows OS**. Par contre, ces outils ne s'exécuteront que si les virus qui infectent votre ordinateur ne les empêchent pas de fonctionner normalement.

- [HijackThis](#) [19] et d'autres outils gratuits [Clean-up Tools](#) [20] de la compagnie **Trend Micro**.
- [RootkitRevealer](#) [21] de [Sysinternals](#) [22] de **Microsoft**.

**Commentaire:** Il est possible d'utiliser les outils listés ci-dessus séparément pour maximiser vos chances de nettoyer votre ordinateur complètement.

### Méthode B: Réinstaller le système d'exploitation Windows de Microsoft

**Commentaire:** Avant d'entamer le processus de réinstallation, assurez-vous de disposer de tous les numéros de série et licences nécessaires, ainsi que des copies d'installation de **Windows OS** et de tous les programmes dont vous avez besoin. Ce processus peut prendre un certain temps mais en vaut l'effort si vous n'avez pas réussi à éliminer toutes les menaces avec les autres méthodes.

Dans de rares cas, une infection peut s'avérer tellement destructrice que les logiciels recommandés ci-dessus s'avèrent impuissants. Dans de telles situations, il est recommandé de suivre les étapes énumérées ci-dessous:

1. Créer une copie de sauvegarde de tous vos fichiers personnels.
2. Réinstaller le système d'exploitation **Microsoft Windows** en formatant le disque au complet.
3. Mettre à jour le système d'exploitation **Microsoft Windows** immédiatement après l'installation.
4. Installer **avast!** (ou un autre programme antivirus recommandé) et le mettre à jour.
5. Installer tous les programmes dont vous avez besoin et télécharger les plus récentes versions, ainsi que toutes les mises à jour pour chaque programme.

**IMPORTANT:** Vous ne devriez *jamais* insérer votre disque de sauvegarde dans le lecteur de votre ordinateur avant d'avoir complété toutes ces tâches. Vous risqueriez ainsi de ré-infecter votre ordinateur.

6. Insérez votre copie de sauvegarde dans le lecteur de l'ordinateur et exécutez un scan minutieux pour détecter et éliminer tous les problèmes potentiels.
7. Lorsque vous aurez détecté et supprimé tous les problèmes, vous pourrez copier vos fichiers du disque de sauvegarde vers votre disque dur.

## Faq et questions récapitulatives

Elena et Nikolai trouvent Avast plutôt facile à utiliser, mais ils ne sont pas encore certains de connaître assez bien le programme et ses fonctionnalités.

**Q:** Comment puis-je m'assurer que mes documents ne seront pas infectés si j'utilise un ordinateur dans un café Internet, et qu'aucun programme antivirus n'est installé sur cet ordinateur?

**A:** Excellente question! Il est bon de constater que tu te rends compte à quel point les virus peuvent s'avérer dangereux. L'utilisation d'ordinateurs publics comporte un facteur de risque élevé. On ne sait jamais quel type de programmes malveillants peuvent s'y trouver. Voici un conseil simple : ne jamais utiliser d'ordinateurs publics pour effectuer des tâches importantes ou délicates, à moins de n'avoir absolument aucune alternative.

**Q:** J'ai plusieurs ordinateurs et une connexion Internet plutôt lente. Comment puis-je télécharger la mise à jour des définitions de virus pour tous mes ordinateurs?

**A:** Tu peux **télécharger les plus récentes mises à jour** [23] directement du site Internet d'avast!, puis les distribuer à chaque ordinateur de ton réseau.

**Q:** Qu'advient-il des fichiers qui se trouvent dans la Zone de quarantaine si je désinstalle **avast!**?

**A:** Tous les fichiers contenus dans la Zone de quarantaine seront supprimés si tu désinstalles le programme.

### 5.1 Questions récapitulatives

- Comment peut-on scanner un répertoire en particulier avec **avast!**?
- Combien de jours peut-on utiliser **avast!** avant de devoir l'enregistrer?
- Est-il possible de déplacer un document qui n'est pas infecté par un virus vers la *Zone de quarantaine*?
- Quelle est la différence entre supprimer un virus et le déplacer vers la *Zone de quarantaine*?
- Quelle est la différence entre un scan au démarrage et un scan minutieux du système?

## Spybot - anti-mouchard

### Short Description:

**Spybot Search & Destroy** est utilisé pour détecter et éliminer divers types de logiciels publicitaires (*adware*), malveillants (*malware*) ou espions (*spyware*). Le programme offre des mises à jour gratuites et vous permet d'immuniser votre navigateur Internet contre des infections futures.

### Online Installation Instructions:

#### Pour télécharger Spybot

- Lisez la courte **introduction** aux **Guides pratiques** <sup>[1]</sup>.
- Cliquez sur l'icône **Spybot** ci-dessous pour ouvrir la page de téléchargement <http://www.safer-networking.org/fr/mirrors/index.html>
- Choisissez une source de téléchargement parmi celles listées sur cette page en cliquant sur le bouton "**Téléchargement ici**".
- Téléchargez le programme d'installation. Ensuite, trouvez-le et cliquez dessus.
- Si vous avez sauvegardé l'exécutable de **Spybot** sur votre ordinateur, vous pouvez le supprimer après l'installation.

### Spybot:



[24]

### Site Internet

[www.safer-networking.org/fr](http://www.safer-networking.org/fr) <sup>[25]</sup>

### Configuration requise

- Compatible avec toutes les versions de Windows

### Version utilisée pour rédiger ce guide

- 1.6.2

### Licence

- Gratuitiel (*Freeware*)

### Lecture requise

- Livret pratique Security in-a-box, chapitre **1. Protéger votre ordinateur contre les logiciels malveillants et les pirates** <sup>[4]</sup>

**Niveau:** 1: Débutant, 2 : Moyen, 3 : Intermédiaire, 4 : Expérimenté, 5 : Avancé

**Temps d'apprentissage:** 20 minutes

### Ce que vous apportera l'utilisation de cet outil:

- La capacité de **supprimer** plusieurs types de logiciels malveillants et/ou espions.
- La capacité de **vacciner** votre système informatique **avant** qu'il ne soit infecté ou menacé de perturbations malveillantes.

### Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

Les systèmes d'exploitation **GNU Linux** et **Mac OS** sont, à l'heure actuelle, pratiquement épargnés par les logiciels malveillants (mouchards, virus, etc.). Pour vous protéger, nous vous recommandons de: **1)** mettez régulièrement à jour votre système d'exploitation, ainsi que tous les programmes qui y sont installés; **2)** utilisez un des programmes antivirus listés au chapitre portant sur *Avast* <sup>[26]</sup>; **3)** utilisez un des programme pare-feu listés au chapitre portant sur *Comodo* <sup>[27]</sup>; **4)** utilisez un navigateur sûr comme *Firefox* <sup>[28]</sup> avec le module complémentaire *[NoScript]* (*/fr/firefox\_noscript*) qui empêche l'exécution des scripts téléchargés automatiquement avec les pages web. Ces mesures préventives suffiront à protéger votre système **GNU Linux** ou **Mac OS**.

La situation est très différente pour les ordinateurs équipés du système **Microsoft Windows**. Des milliers de nouveaux logiciels malveillants sont conçus chaque jour. Les méthodes d'attaque sont de plus en plus sophistiquées. Les mesures préventives décrites au précédent paragraphe sont **nécessaires** aux ordinateurs qui fonctionnent avec **Microsoft Windows**. De plus, nous recommandons fortement l'utilisation de **Spybot**, telle que décrite dans le présent chapitre. Si malgré toutes ces précautions votre ordinateur est infecté et que vous avez besoin d'outils supplémentaires, nous recommandons les logiciels suivants:

1. Installez **SuperAntiSpyware** <sup>[29]</sup>, actualisez les définitions et scannez votre ordinateur.
2. Installez **Malwarebytes Anti-Malware** <sup>[30]</sup>, lancez un *Scan rapide*, puis lancez un *Scan*. Lorsque l scan est complété, supprimez les mouchards détectés affichés dans le panneau *Show Results*
3. Utilisez d'autres programmes anti-mouchards gratuits comme: **Microsoft Windows Defender** <sup>[31]</sup>, **Ad-Aware Internet Security** <sup>[32]</sup> ou **SpywareBlaster** <sup>[33]</sup>.

### 1.1 À propos de cet outil

**Spybot S&D** est un programme libre et gratuit, dont l'usage est très répandu pour détecter et éliminer des systèmes informatiques divers types de logiciels publicitaires (*adware*), malveillants (*malware*) ou espions (*spyware*). Le programme vous permet également de vacciner votre système contre les logiciels publicitaires, malveillants et/ou espions avant même qu'ils n'infectent votre ordinateur.

Le terme « logiciel publicitaire » (ou publiciel; *adware* en anglais) désigne tout logiciel qui affiche des publicités sur votre ordinateur. Certains types de publiciels fonctionnent sensiblement comme des logiciels espions et peuvent envahir votre vie privée ou menacer la sécurité de votre système.

Le terme « logiciel malveillant » (*malware* en anglais) désigne tout programme – par ex. des Chevaux de Troie (*Trojans*) ou des vers informatiques (*worms*) – conçu pour nuire à votre ordinateur ou en détourner les opérations sans votre consentement, ou sans même que vous en soyez conscient.

Le terme « logiciel espion » (ou mouchard; *spyware* en anglais), désigne tout programme conçu pour récolter des données, observer et enregistrer vos renseignements privés et surveiller vos habitudes de navigation sur Internet. Tout comme les logiciels malveillants, les mouchards s'exécutent souvent sur votre ordinateur à votre insu. C'est pourquoi l'installation d'un programme comme **Spybot** vous aidera à protéger votre système et à VOUS protéger!

**Spybot** installe aussi une application supplémentaire appelée **TeaTimer**. Cela protégera votre ordinateur contre d'éventuelles infections par des logiciels malveillants.

**Commentaire:** **Windows Vista** comporte son propre programme anti-espion, appelé **Windows Defender**. **Vista** semble cependant laisser **Spybot** fonctionner sans conflit.

#### Offline Installation Instructions :

#### Pour installer SpyBot

- \*Lisez la courte **Introduction** aux **Guides pratiques** <sup>[1]\*\*</sup>
- **Cliquez sur l'icône SpyBot ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.

SpyBot:



[34]


## Comment installer et utiliser Spybot

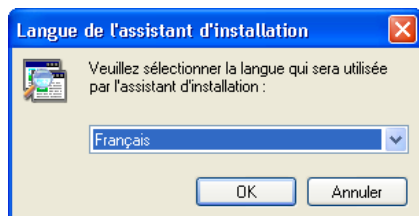
Sommaire des sections de cette page:

- [2.0 Comment installer Spybot](#)
- [2.1 À propos de Spybot](#)
- [2.2 Comment utiliser Spybot pour la première fois](#)
- [2.3 Comment actualiser les règles de détection et les bases de données de vaccination de Spybot](#)
- [2.4 Comment vacciner votre système](#)
- [2.5 Comment détecter la présence de problèmes](#)
- [2.6 Le Résident TeaTimer](#)
- [2.7 Comment utiliser l'outil de Sauvegardes](#)

---

## 2.0 Comment installer Spybot

**Première étape.** Double-cliquez sur  *spybot162.exe*; si la boîte de dialogue *Fichier ouvert - Avertissement de sécurité* s'affiche, cliquez sur  pour afficher la fenêtre suivante:



\*Figure 1: La fenêtre Langue de l'assistant d'installation \*

**Deuxième étape.** Cliquez sur  pour afficher la fenêtre *Installation - Spybot Search & Destroy – Bienvenue dans l'assistant d'installation de Spybot - Search & Destroy*.

**Troisième étape.** Cliquez sur  pour afficher la fenêtre *Accord de licence*. Veuillez lire l'*Accord de licence* avant de poursuivre le processus d'installation.

**Quatrième étape.** Cochez l'option *Je comprends et j'accepte les termes du contrat de licence* pour activer le bouton *Suivant*, puis cliquez sur  pour afficher la fenêtre *Dossier de destination*.

**Cinquième étape.** Cliquez sur  pour afficher la fenêtre suivante:

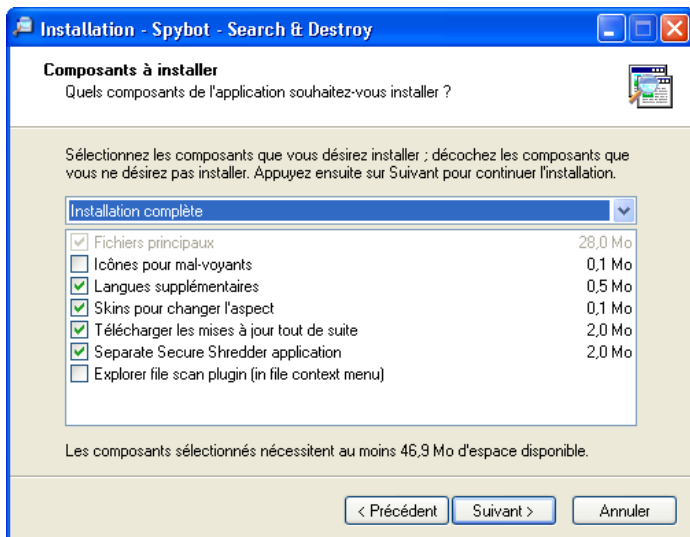







Figure 2: La fenêtre Composants à installer

**Sixième étape.** Cochez les composants appropriés pour que la fenêtre correspondent à la figure 2 ci-dessous, puis cliquez sur  pour afficher la fenêtre *Sélection du dossier de menu Démarrer*.

**Septième étape.** Cliquez sur  pour accepter l'emplacement par défaut et afficher la fenêtre *Tâches supplémentaires*.

**Huitième étape.** Cliquez sur  pour afficher la fenêtre *Prêt à installer*, puis cliquez sur  pour afficher la fenêtre *Installation en cours*.

**Neuvième étape.** Cliquez sur  pour finaliser le processus d'installation et lancer **Spybot - Search & Destroy**.

## 2.1 À propos de Spybot

L'utilisation appropriée de **Spybot** comporte deux étapes élémentaires:

- Mettre à jour les *Règles de détection (Detection Rules)* et les *Bases de données de vaccination (Immunization databases)* avec l'information la plus récente et la plus pertinente.
- Exécuter **Spybot**. Cela implique la vaccination de votre système avec les règles de détection et les bases de données de vaccination que vous avez préalablement téléchargées, la vérification du système afin de détecter tout logiciel malveillant ou espion qui pourrait s'y trouver et, finalement, l'élimination des infections trouvées.

**Note:** Pour un aperçu des fonctions avancées, veuillez consulter la section **3.0 Mode avancé** <sup>[35]</sup>.

## 2.2 Comment utiliser Spybot pour la première fois

Lorsque vous aurez finalisé l'installation, **Spybot** affichera automatiquement la fenêtre Infos légales illustrée ci-dessous:

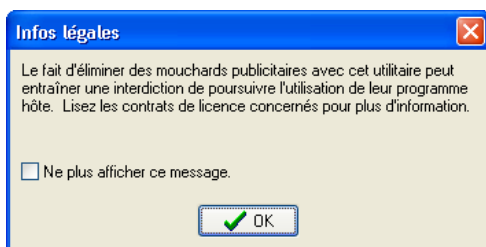




Figure 3: La fenêtre Infos légales

**Commentaire:** Pour lancer **Spybot** la prochaine fois, vous pouvez, soit double-cliquer sur  ou sélectionner **Démarrer > Programmes > Spybot - Search & Destroy > Spybot - Search & Destroy**.

**Première étape.** Cliquez sur  pour afficher la console *Spybot - Search & Destroy* (figure 8) et la fenêtre *Créer une sauvegarde du Registre*, tel qu'illustré ci-dessous:

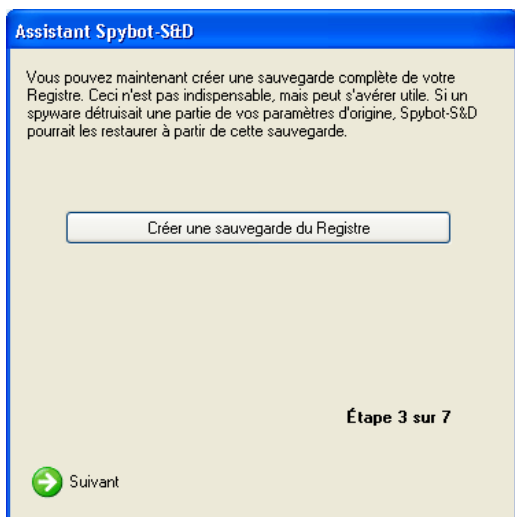


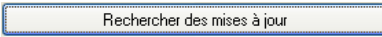


Figure 4: La fenêtre Créer une sauvegarde du Registre de l'Assistant Spybot-S&D

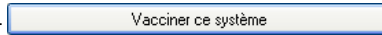
**Commentaire:** Il est fortement conseillé de créer une copie de sauvegarde du registre. L'explication détaillée du **Registre Windows** est donnée dans le guide pratique **CCleaner** [36].

**Deuxième étape.** Cliquez sur  dans la figure 4 pour créer et sauvegarder une copie de sauvegarde du registre de votre système.

**Troisième étape.** Cliquez sur  pour afficher la fenêtre *Spybot – Rechercher des mises à jour*. Si vous êtes connecté à Internet, suivez les étapes énumérées ci-dessous:

**Quatrième étape.** Cliquez sur  pour afficher la fenêtre *Spybot – Rechercher des mises à jour*, et rendez-vous directement à la section **Comment actualiser les règles de détection et les bases de données de vaccination de Spybot**.

- Si vous n'êtes pas connecté à Internet, suivez les étapes énumérées ci-dessous:

**Cinquième étape.** Cliquez sur  pour afficher la fenêtre *Vaccination du système*, et lancer la vaccination du système, tel qu'illustré ci-dessous:

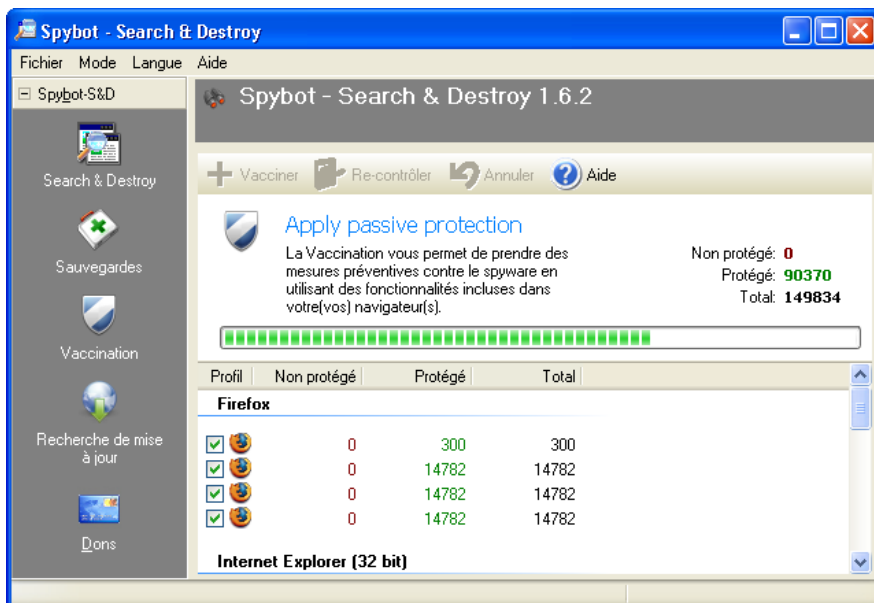


Figure 5: Le processus de vaccination en cours

**Commentaire:** Si vous avez laissé une page de navigateur ouverte, la fenêtre suivante s'affichera avant que le processus de vaccination se mette en marche:



Figure 6: The Open Browser Detected screen

**Sixième étape.** Fermez votre navigateur, puis cliquez sur  pour vacciner votre système.

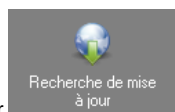
**Septième étape.** Cliquez sur  , puis cliquez sur  pour revenir à la console de *Spybot - Search & Destroy* en mode *Vaccination*.



Figure 8: La console Spybot - Search & Destroy

## 2.3 Comment actualiser les règles de détection et les bases de données de vaccination de Spybot

**Important:** Il est crucial que vous mainteniez **Spybot** à jour avec les plus récentes définitions.




**Première étape.** Cliquez sur  dans le menu de gauche de *Spybot-S&D* pour afficher la fenêtre *Spybot-S&D Mise à jour* présentant une liste de serveurs d'où il est possible de télécharger les mises à jour.


**Deuxième étape.** Choisissez l'emplacement le plus rapproché de votre lieu de résidence, puis **cliquez à droite** et **sélectionnez** l'option *Positionner ce serveur comme miroir préféré* tel qu'illustré à la *figure 9* ci-dessous.

- Si vous avez effectué la mise à jour des règles de détection récemment, une fenêtre apparaît pour vous aviser qu'**Aucune mise à jour n'est disponible**.
- Si vous n'avez pas effectué la mise à jour des règles de détection récemment, la fenêtre de *Mises à jour de Spybot-S&D* apparaît, affichant une liste de serveurs d'où il est possible de télécharger les mises à jour ::



Figure 9: La fenêtre Spybot-S&D Mise à jour

**Troisième étape.** Cliquez sur  pour afficher la fenêtre Spybot-S&D Mise à jour - Veuillez choisir les mises à jour à télécharger ici.

**Quatrième étape.** Cochez toutes les options présentées, puis cliquez sur  pour lancer le téléchargement de ces mises à jour.

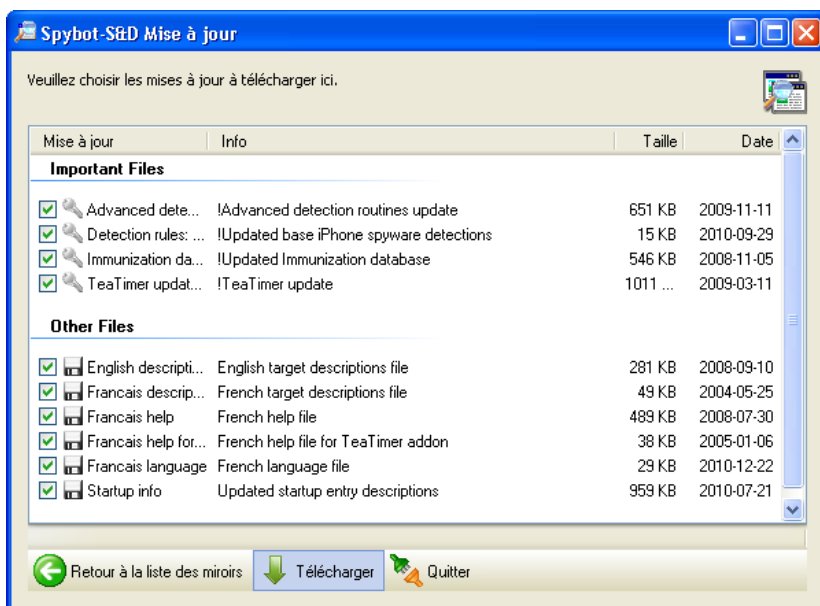


Figure 10: La fenêtre de mise à jour de Spybot-S&D affichant les règles de détection, les fichiers d'aide et les bases de données de vaccination

**Commentaire:** Si une erreur se produit pendant le téléchargement de ces mises à jour, Spybot vous donnera l'occasion de réessayer. Après avoir terminé le téléchargement avec succès, le programme vous invitera à vacciner votre système et à vérifier s'il comporte des problèmes:

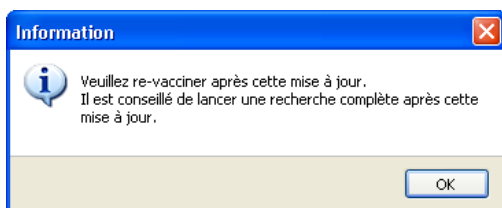


Figure 11: La fenêtre Information

**Sixième étape.** Cliquez sur , puis sur .

Vous serez alors redirigé vers la fenêtre principale de Spybot - Search & Destroy

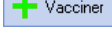
**Commentaire:** Vous pouvez également exécuter le processus de mise à jour de Spybot en tout temps en: **Sélectionnant : Démarrer > Programmes > Spybot Search & Destroy > Update Spybot S&D.**

## 2.4 Comment vacciner votre système


**Spybot** contribue à protéger votre ordinateur contre les logiciels malveillants et les mouchards identifiés en procédant à sa "vaccination". C'est un exercice similaire à la vaccination que nous recevons pour nous prémunir contre les maladies infectieuses.

Pour vacciner votre système informatique, suivez les étapes énumérées ci-dessous :



**Première étape.** Cliquez sur **Vaccination** dans le menu **Spybot-S&D** ou  pour automatiquement lancer le processus de vaccination, tel qu'illustré à la *figure 6* ci-dessus.

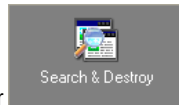
Vous devrez peut-être agrandir la fenêtre pour afficher toutes les options du panneau *Vaccination*.

**Commentaire:** Il est possible de renverser ou défaire le processus de vaccination si vous craignez que la vaccination du système ait eu un effet négatif sur la performance de votre ordinateur. Vous pouvez cliquer sur  pour renverser le processus de vaccination et restaurer votre système à son état précédent.

## 2.5 Comment détecter la présence de problèmes

**Rappel:** Avant de commencer à vérifier votre système pour y détecter de potentielles menaces, il est important d'actualiser les *règles de détection* et les *bases de données de vaccination* de **Spybot**.

Pour contrôler la présence de problèmes et de menaces, suivez les étapes ci-dessous:



**Première étape.** Cliquez sur **Search & Destroy** pour afficher le panneau de **Spybot Search and Destroy**.



**Deuxième étape.** Cliquez sur **Vérifier tout** pour entamer la vérification du système et y détecter d'éventuelles menaces (si vous avez un gros volume de données, de fichiers et de programmes, etc., cette étape peut prendre entre 20 minutes et une heure). Il est possible qu'une fenêtre d'invite comme celle-ci s'affiche :



Figure 12: Le programme *Spybot - S&D* vérifiant le système pour y détecter des problèmes.

**Troisième étape.** Cliquez sur  pour entamer la vérification du système:

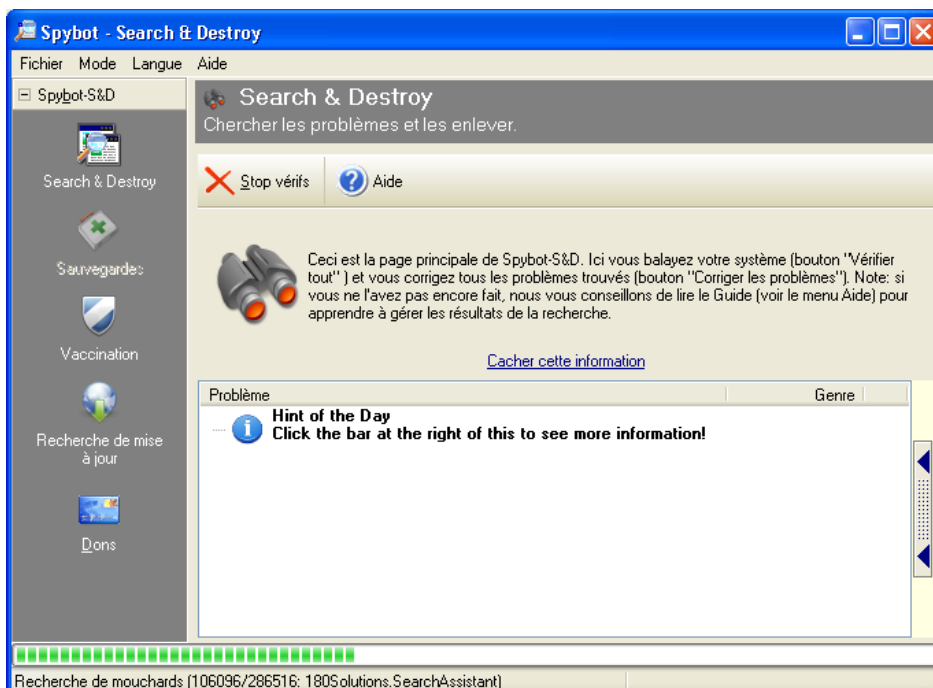




Figure 13: Le programme Spybot - S&D vérifiant le système pour y détecter des problèmes.

Lorsque la vérification est achevée, le nombre et la nature des problèmes est listée dans le panneau principal::

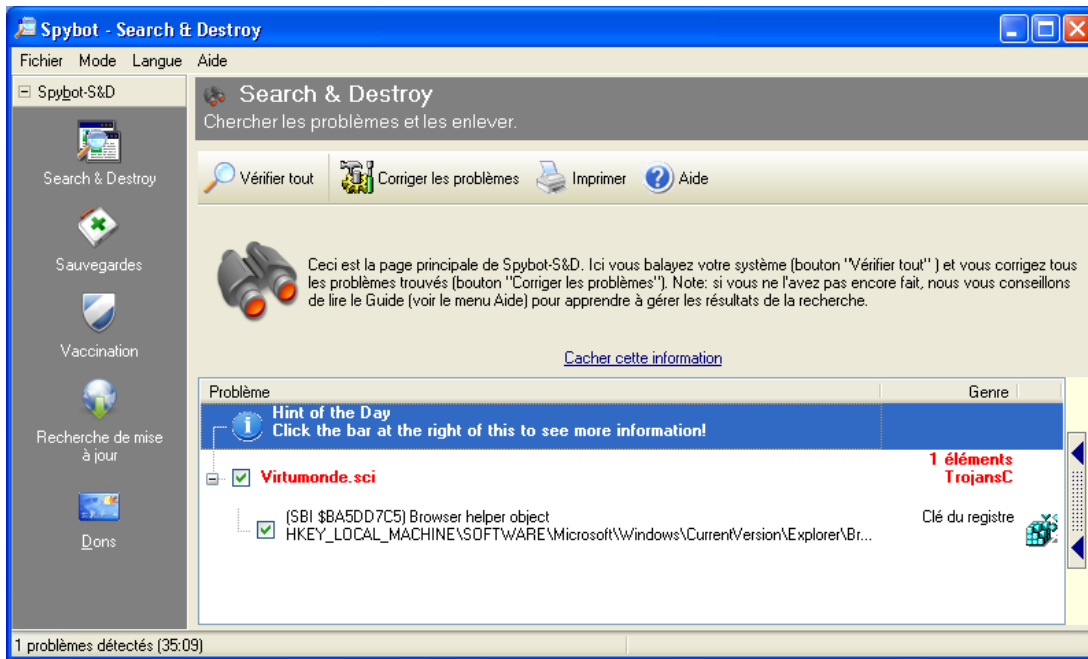



Figure 14: La fenêtre principale de Spybot - S&D affichant les problèmes et menaces potentielles

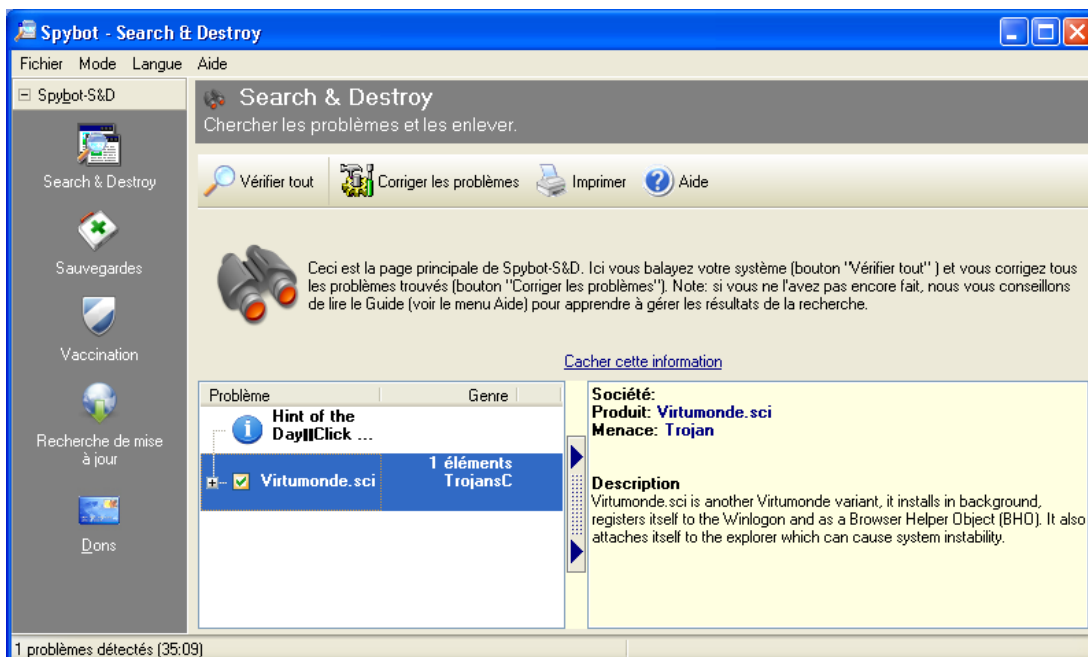
**Quatrième étape.** Ne cochez uniquement que les éléments que vous souhaitez supprimer. Certains des éléments trouvés sont peut-être des logiciels publicitaires que vous souhaitez conserver (pour une raison ou une autre).

**Astuce:** Tous les éléments affichés en lettres rouges sont généralement considérés comme des problèmes ou des menaces. Tous les éléments affichés en lettres vertes servent à surveiller vos habitudes d'utilisation d'Internet. Pour conserver un élément en particulier, décochez la case qui y est associée et cet élément ne sera pas supprimé.

**Important:** Avant de supprimer ou ignorer un logiciel malveillant que vous avez trouvé, il est fortement recommandé d'en examiner le comportement et l'origine.



**Cinquième étape.** Cliquez sur  du côté droit de la fenêtre des résultats de Spybot, pour afficher des renseignements sur l'élément trouvé. Si rien ne s'affiche, vous pouvez effectuer une recherche sur Internet. Renseignez-vous sur le fonctionnement et le comportement de l'élément trouvé et sur comment il peut compromettre l'intégrité et la sécurité de votre système. Une meilleure connaissance des problèmes et des menaces entraîne une plus grande sécurité et une meilleure protection de votre vie privée.



\*Figure 15: Le panneau Afficher plus d'informations de Spybot - S&D \*

**Sixième étape.** Cliquez sur  pour activer la suppression des logiciels malveillants.

Une boîte de dialogue apparaît vous demandant de confirmer que vous souhaitez supprimer tous les problèmes trouvés.

**Septième étape.** Cliquez sur le bouton *oui* si vous souhaitez les supprimer.

**Commentaire:** De façon générale, il est recommandé d'effectuer une vérification du système chaque semaine.

## 2.6 Le Résident TeaTimer

Le **Résident TeaTimer** est un programme de **Spybot** qui tourne constamment en arrière-plan (c.-à-d. même lorsque vous n'êtes pas en train d'utiliser **Spybot**). Le programme surveille continuellement les principaux processus du système pour s'assurer qu'aucune menace potentielle ne modifie les configurations ou les paramètres essentiels du système. **TeaTimer** vous alerte chaque fois qu'un processus suspect ou malveillant est détecté et vous demande d'*autoriser* ou de *refuser* ce processus (si celui-ci s'avère malveillant). Voici un exemple d'alerte de **TeaTimer** :

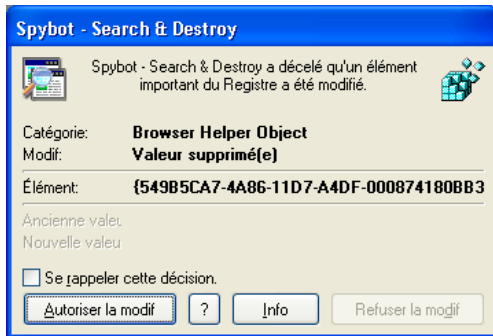


Figure 16: Une alerte du Résident TeaTimer de Spybot - S&D, présentant le choix d'autoriser ou de refuser le changement

Étant donné que plusieurs programmes (qu'ils soient nécessaires ou malveillants) exigent un accès aux processus internes du système, **TeaTimer** vous demandera régulièrement d'*autoriser* ou de *refuser* des changements. Dans cet exemple, **Skype** est supprimé du menu de Démarrage de Windows. Cela se produit habituellement lorsque vous désinstallez un programme (et pas nécessairement uniquement lors du démarrage). Dans ce cas, il s'agit d'une requête valide concernant une modification mineure à un paramètre du système et vous pouvez donc l'autoriser.

**Astuce:** Si vous n'êtes pas certain de comprendre l'alerte de **TeaTimer** et aimeriez obtenir un supplément d'information, cliquez sur .



Figure 17: La fenêtre de démarrage de Spybot - Search & Destroy

Il est plus sûr de refuser une requête si vous n'êtes pas certain de l'action posée. Par contre, si vous êtes certain que la requête est légitime, cocher la case *Se rappeler de cette décision* et **Spybot** n'affichera plus cette alerte à l'avenir.

**Commentaire:** Vous verrez souvent TeaTimer s'activer lorsque vous installez un nouveau programme et que celui-ci tente de s'ajouter au processus de démarrage. La même chose se produit lorsque vous désinstallez un programme.

**Astuce:** Il est fortement recommandé d'actualiser TeaTimer chaque fois que des mises à jour sont disponibles.

## 2.7 Comment utiliser l'outil de Sauvegardes

L'outil de *Sauvegardes* permet de récupérer ou de retrouver chaque élément précédemment supprimé ou réparé. Cela est possible car **Spybot** crée une copie de sauvegarde pour chaque élément supprimé. Si un logiciel malveillant est supprimé et que cela entraîne une défaillance de l'ordinateur, il est possible de récupérer l'élément en question en utilisant l'outil de *Sauvegardes*.

Pour récupérer un élément précédemment supprimé, suivez les étapes énumérées ci-dessous :



**Première étape.** Cliquez sur  pour afficher la fenêtre de *Sauvegardes* illustrée ci-dessous :

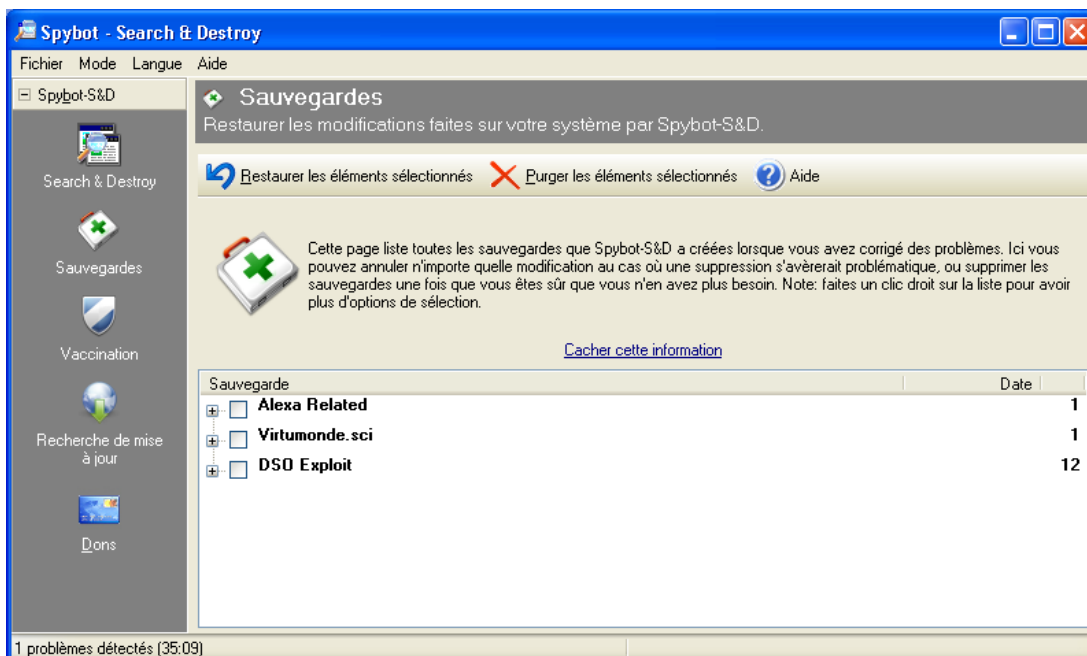


Figure 18: La fenêtre de sauvegardes de Spybot - Search & Destroy

**Deuxième étape.** Dans la liste des éléments précédemment supprimés, **cochez** les éléments que vous souhaitez récupérer, puis **cliquez** sur .

Une boîte de dialogue de confirmation est alors activée:

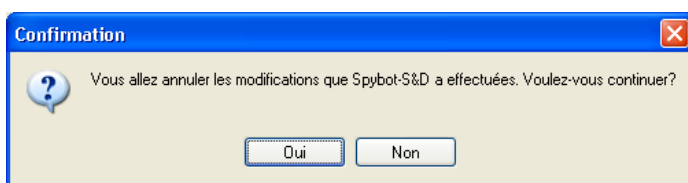



Figure 19: La boîte de dialogue de confirmation

**Troisième étape.** Cliquez sur  pour récupérer ces éléments.

**Quatrième étape.** Autrement, cliquez sur  pour éliminer définitivement les éléments cochés. Cependant, soyez conscient que les éléments purgés ne seront plus récupérables.

## Comment utiliser Spybot en mode avancé

- [3.0 À propos du mode avancé](#)
- [3.1 Comment activer le mode avancé](#)
- [3.2 Comment utiliser les outils du mode avancé](#)

### 3.0 À propos du mode avancé\*

Spybot fonctionne en mode *par défaut* et en mode *avancé*. Le mode *avancé* vous permet d'accéder aux paramètres du programme, ainsi qu'à des outils supplémentaires.

#### 3.1 Comment activer le mode avancé

Pour activer le mode *avancé* de **Spybot**, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez **Mode > Mode avancé** dans la barre menu:

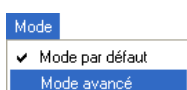


Figure 1: Les options du sous-menu Mode

Cette action activera la fenêtre suivante:

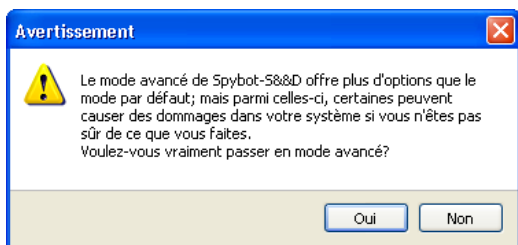


Figure 2: La fenêtre d'invite Avertissement

Deuxième étape. Cliquez sur  pour confirmer le choix du mode avancé.

Dans le mode avancé, le menu latéral de **Spybot** comporte plus d'options que sous le mode par défaut:



Figure 3: Le menu latéral du mode avancé de Spybot - Search & Destroy

Troisième étape. Double-cliquez sur **Réglages** pour afficher les descriptions de divers éléments et options dans le panneau principal:



Figure 4: La fenêtre réglages

Quatrième étape. Double-cliquez sur **outils** pour afficher les outils qui vous permettront d'identifier des mouchards que le processus de vérification normal ne suffit pas à détecter, et à refaire la vérification du système.

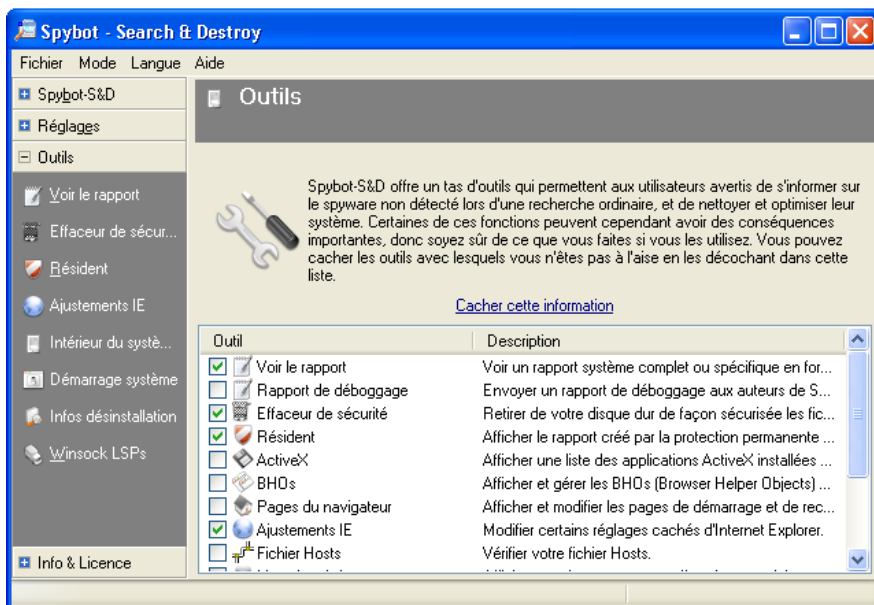


Figure 5: La fenêtre outils

**Cinquième étape.** Double-cliquez sur *Info & Licence* pour afficher les renseignements généraux et l'information portant sur la licence d'utilisation de **Spybot 1.6.2**.

## 3.2 Comment utiliser les outils du mode avancé

Les utilisateurs **avancés** apprécieront les options avancées offertes par **Spybot**: *Ajustements IE*, *Effaceur de sécurité*, *Intérieur du système* et *Démarrage système*.

### 3.2.1 Ajustements IE

L'option *Ajustements IE* sert à la configuration d'**Internet Explorer**. Cela vous permet de configurer certains paramètres de sécurité importants d'IE, en particulier lorsque plusieurs utilisateurs se servent d'un même système.



Figure 6: La fenêtre Ajustements IE

Vous devriez toujours laisser la première option cochée, tel qu'illustré dans l'exemple ci-dessus.

### 3.2.2 Effaceur de sécurité

Voici une option très pratique pour supprimer définitivement (effacer) des fichiers temporaires de **Windows** et du navigateur Internet. Pour plus d'information sur la suppression définitive de fichiers temporaires, consultez le chapitre **6. Détruire définitivement des données sensibles** <sup>[37]</sup> du livre pratique Security in-a-Box.

**Première étape.** Cliquez sur  *Effaceur de sécurité* pour afficher la fenêtre suivante:

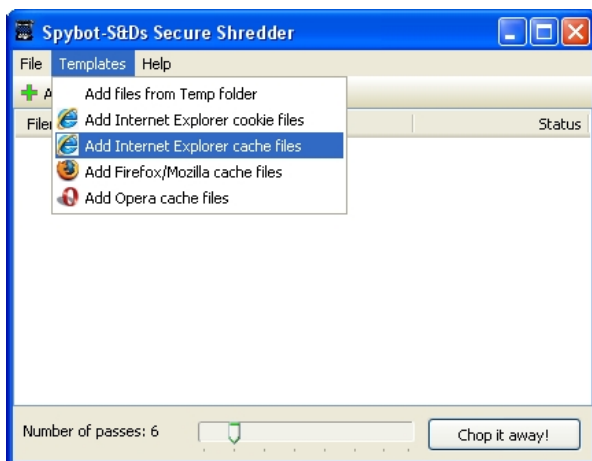


Figure 7: La fenêtre de l'Effaceur de sécurité de Spybot-S&D

**Deuxième étape.** Cliquez sur *Templates* pour activer un menu défilant des emplacements où se trouvent des fichiers temporaires, tel qu'illustré à la figure 7, puis **sélectionnez** un item dans la liste pour remplir la fenêtre de l'Effaceur de sécurité de Spybot-S&D:

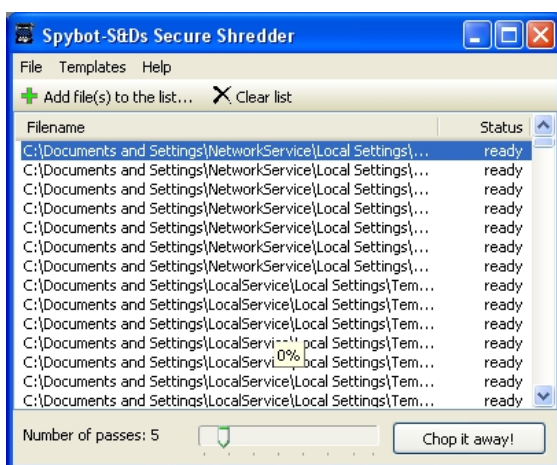


Figure 8: La liste des fichiers temporaires dans la fenêtre de l'Effaceur de sécurité

**Troisième étape.** Sélectionnez un ou des fichier(s) à supprimer.

**Quatrième étape\*.** Déterminer le nombre de passages utilisés pour effacer le(s) fichier(s) sélectionné(s):

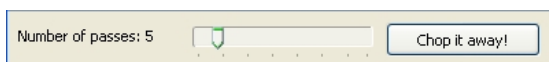


Figure 9: Choisissez le nombre de passages désiré

**Cinquième étape.** Cliquez sur **Chop it away!** après avoir déterminé le nombre de passages que comptera la processus de suppression

**Spybot supprimera définitivement de votre ordinateur tous les fichiers temporaires non nécessaires.**

Vous pouvez également utiliser l'Effaceur de sécurité pour supprimer et effacer d'autres fichiers. Pour ce faire, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez > **Add file(s) to the list...** pour afficher la fenêtre suivante:

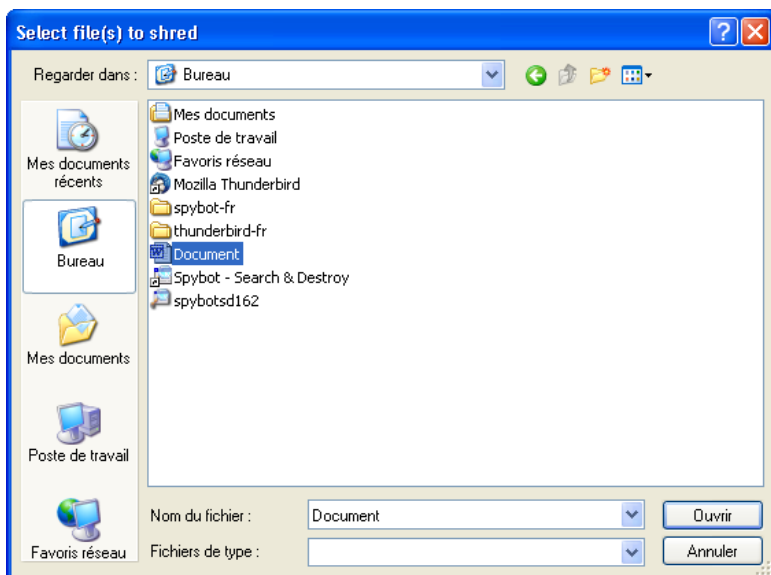




Figure 10: La fenêtre de navigateur Select File(s) to shred

**Deuxième étape.** Sélectionnez le fichier que vous souhaitez effacer.

**Troisième étape.** Cliquez sur  pour afficher le fichier dans la *figure 8*, puis cliquez  sur (/sbox/screen/spybot-fr/61.png) pour supprimer et effacer le fichier.

### 3.2.3 Intérieur du système (Pour utilisateurs avancés seulement!)

L'outil *Intérieur du système* cherchera des fichiers incorrectement nommés ou dotés de noms incohérents dans le **Registre Windows**. L'explication détaillée du registre de Windows est donnée dans le Guide pratique **CCleaner** <sup>[36]</sup>.

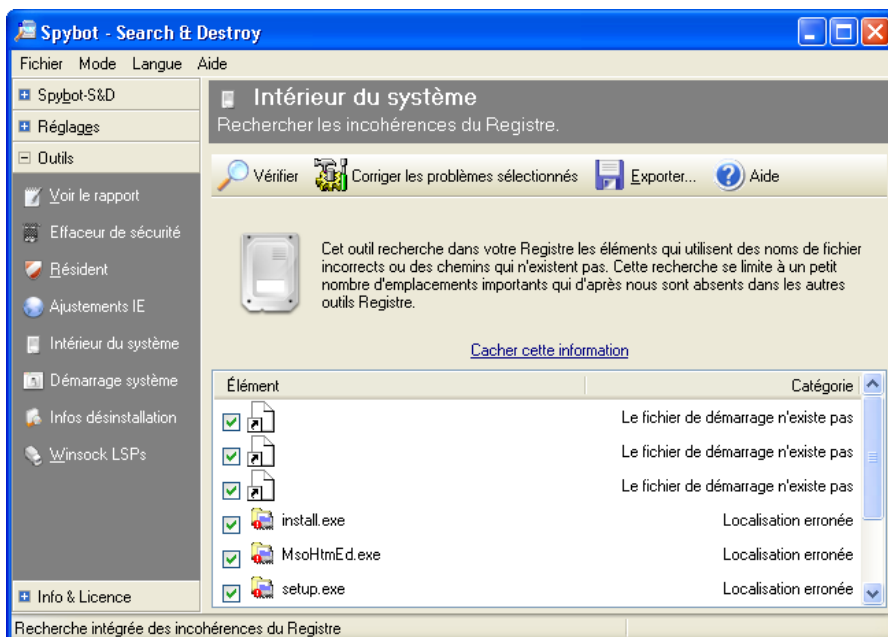



Figure 11: La fenêtre Intérieur du système

**Première étape.** Cliquez sur  pour entamer la recherche de problèmes dans le **Registre Windows**.

**Deuxième étape.** Lorsque la vérification est terminée, cliquez sur  pour corriger tous les problèmes trouvés.

### 3.2.4 Démarrage système (Pour utilisateurs avancés seulement!)

L'outil *Démarrage système* affiche, en ordre séquentiel, tous les programmes chargés par **Windows** au démarrage de l'ordinateur. Il vous laisse départager ceux qui sont nécessaires de ceux qui ne sont pas essentiels au démarrage.

**Astuce:** Le retrait de certains éléments de cette liste augmente la vitesse à laquelle **Windows** démarre.

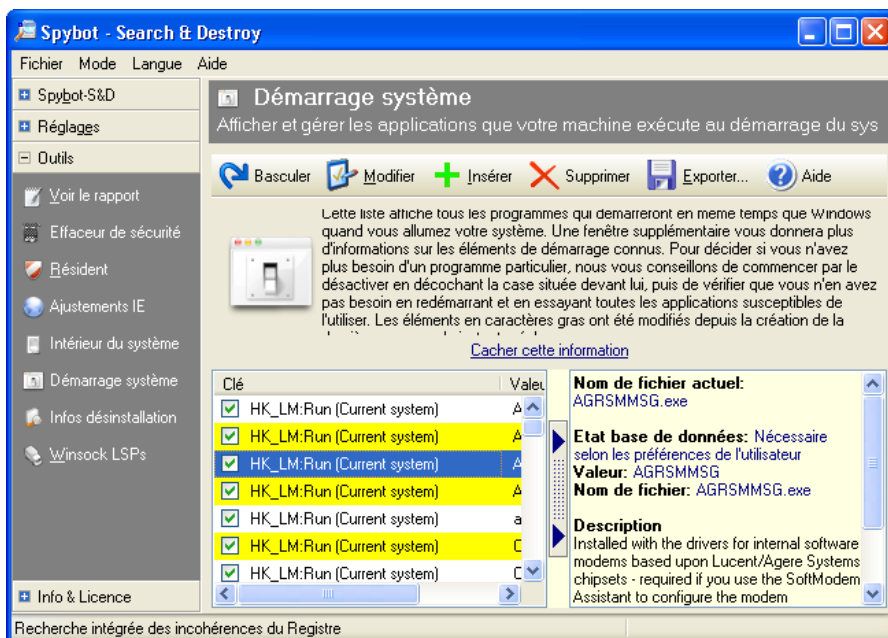
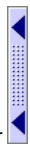


Figure 12: La fenêtre de l'outil Démarrage système



Première étape. Cliquez sur  pour afficher le panneau d'information.

Dans ce panneau d'information, chaque élément surligné comporte une description de son comportement et de sa fonction. Lisez attentivement ces descriptions avant de décider si oui ou non un élément doit être chargé au démarrage de Windows.

## Faq et questions récapitulatives

### 4.0 Faq et questions récapitulatives

Elena et Nikolai ont tous deux l'impression que Spybot est un programme complet et facile à utiliser. Sa fonction essentielle, soit de protéger un ordinateur des infections et des mouchards, est exécutée automatiquement. Même s'ils sont un peu nerveux d'autoriser ou de refuser certains changements lorsque **TeaTimmer** sollicite leur attention, ils ont le sentiment qu'ils apprendront rapidement à différencier les processus légitimes des processus malveillants.

**Q:** Si je désinstalle le programme, qu'advient-il des programmes espions que **Spybot** a trouvé lors des recherches effectuées dans le passé? Demeurent-ils "en quarantaine" sur mon ordinateur, ou sont-ils en fait supprimés?

**A:** Lorsque tu désinstalles **Spybot**, tous les éléments placés en quarantaine sont supprimés.

**Q:** Nikolai, je perd souvent la trace de cookies et de trackers dont j'ai besoin ou que je trouve utiles. Comment puis-je empêcher qu'ils soient supprimés ou réparés?

**A:** Ne t'en fais pas. Il y a plusieurs façons de protéger tes cookies utiles. Premièrement, lorsque **Spybot** a achevé la vérification du système, il dresse une liste de tous les problèmes et de toutes les menaces détectés. **Clique** sur chacun des éléments pour obtenir des renseignements supplémentaires à leur sujet et pour t'aider à décider si tu souhaites bel et bien le supprimer, ou au contraire le garder. Sinon, lance **Spybot** et **sélectionne Mode > mode avancé > Réglages**. Là, tu peux préciser quels sont les éléments ou les types d'éléments que tu souhaites exclure des missions de recherche et de destruction.

**Q:** Est-il facile de désinstaller **Spybot**?

**A:** \*En fait, c'est assez simple. Tu n'as qu'à **sélectionner > Démarrer > Programmes > Spybot – Search & Destroy > Uninstall Spybot S&D**.

**Q:** Ma connexion Internet est plutôt lente. Comment puis-je optimiser la vitesse de téléchargement des mises à jour des règles de détection et des bases de données de vaccination?

**A:** \*Assure-toi de sélectionner les mises à jour qui correspondent à la région du monde où tu te trouves. Il n'y a aucune raison pour télécharger des mises à jour depuis un serveur qui se trouve en Asie si tu es toi-même quelque part en Europe, d'autant plus si tu dois économiser la bande passante. Les régions sont clairement indiquées par des petits drapeaux, tu devrais facilement pouvoir trouver un serveur près de chez-toi.

**Q:** Pourquoi **Spybot** n'effectue-t-il pas des mises à jour automatiques des règles de détection et des bases de données de vaccination, directement au démarrage du programme?

**A:** Les mises à jour sont automatiques avec les versions réseau et professionnelle de **Spybot**. Puisque tu utilises une version gratuite, certaines fonctionnalités ne sont pas offertes. De toute façon, la mise à jour manuelle des règles de détection et des bases de données de vaccination de **Spybot** est relativement simple et facile. Voici une animation Flash pratique qui montre comment procéder à la mise à jour manuelle du système : [www.safer-networking.org](http://www.safer-networking.org) [38].



## 4.1 Questions récapitulatives

- Qu'est-ce qu'un logiciel malveillant et comment un tel logiciel peut-il affecter mon ordinateur?
- Quel est l'utilité de **TeaTimer**?
- Lorsqu'on supprime un élément avec **Spybot**, est-il possible de le récupérer par la suite?
- À part chercher et détruire des logiciels malveillants, quelles sont les autres fonctions de **Spybot**?

## Comodo - pare-feu

### Short Description:

**COMODO Firewall** est un logiciel pare-feu bien connu et réputé. Il est gratuit pour utilisation personnelle. Ce logiciel protège votre ordinateur des connexions non autorisées depuis, et vers, l'Internet. Ce chapitre est conçu pour répondre aussi bien aux besoins des **débutants** qu'à ceux des utilisateurs **avancés**.

### Online Installation Instructions:

#### Pour installer COMODO Firewall

- Lisez la courte introduction aux **Guides pratiques** <sup>[3]</sup>
- Cliquez sur l'icône de **COMODO Firewall** ci-dessous pour ouvrir la page de téléchargement [personalfirewall.comodo.com/free-download.html](http://personalfirewall.comodo.com/free-download.html).
- Cliquez sur le bouton 'Click to download' dans la section 'Download Comodo Firewall for Windows'.
- Cliquez sur 'Enregistrer le fichier' pour sauvegarder le fichier 'cfw\_installer\_x86.exe' sur votre ordinateur, puis **double-cliquez** sur 'cfw\_installer\_x86.exe' pour lancer l'installation du programme.
- Lisez attentivement la section **2.0 Comment installer COMODO Firewall** avant de continuer.
- Après avoir complété l'installation de **COMODO Firewall** vous pouvez supprimer l'exécutable d'installation de votre ordinateur.

### COMODO:



<sup>[39]</sup>

### Site Internet

[www.personalfirewall.comodo.com](http://www.personalfirewall.comodo.com) <sup>[40]</sup>

### Configuration requise

- Windows 2000/XP/2003/Vista
- Les privilèges d'administration sont nécessaires à l'installation

### Version utilisée pour rédiger ce guide

- 5.0.16

### Licence

- Gratuitiel

### Lecture préalable:

- Livret pratique Security-in-a-Box chapitre **1. Protéger votre ordinateur contre les logiciels malveillants et les pirates** <sup>[4]</sup>

Niveau: 1: Débutant, 2: Moyen, **3: Intermédiaire**, 4: Expérimenté, 5: Avancé

Temps d'apprentissage: 60 minutes

### Ce que vous apportera l'utilisation de cet outil:

- Une protection efficace de votre ordinateur et de votre réseau contre les attaques de tiers hostiles ou de pirates, et contre les programmes malveillants, les virus et autres menaces à vos logiciels et à votre système;
- La capacité, au moyen d'une interface de logiciel aisément configurable, de filtrer toutes les requêtes effectuées par les programmes installés sur votre ordinateur lorsque vous accédez à Internet.

### Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

**GNU/Linux** comporte un pare-feu intégré (**netfilter/iptables** <sup>[41]</sup>) et présente d'excellents paramètres de sécurité. Il existe plusieurs interfaces utilisateurs simplifiées, dont **GUFW** <sup>[42]</sup> (**Graphical Uncomplicated Firewall**) (voir **plus d'information** <sup>[43]</sup>).

**Mac OS** contient également un puissant pare-feu intégré, qui peut être amélioré par un assortiment de modules complémentaires, dont: **NoobProof** <sup>[44]</sup> ou **IPSecuritas** <sup>[45]</sup>. Pour les utilisateurs qui en ont les moyens, nous recommandons l'achat de **Little Snitch** <sup>[46]</sup>, qui permet de pousser au niveau supérieur votre sécurité et la protection de votre identité sur Internet.

À part **COMODO Firewall**, il existe de nombreuses options pour **Microsoft Windows**. Les utilisateurs pourront apprécier **ZoneAlarm Free Firewall** <sup>[47]</sup> ou **Outpost Firewall Free** <sup>[48]</sup>.

### 1.1 À propos de cet outil

Un pare-feu agit comme un portier ou un gardien de votre ordinateur. Le pare-feu applique une série de règles quant à l'information qui doit être autorisée à accéder à votre ordinateur et celle qui doit pouvoir en sortir. Votre pare-feu est le premier programme à recevoir et à analyser l'information provenant d'Internet, et le dernier programme à balayer

l'information sortante.

Le pare-feu permet d'empêcher les pirates ou d'autres intrus d'accéder aux renseignements personnels stockés sur votre ordinateur. Le programme empêche aussi les programmes malveillants d'envoyer de l'information vers Internet sans votre autorisation. **COMODO Firewall** est un logiciel pare-feu bien connu et réputé. C'est un logiciel d'exploitation libre, ce qui signifie que vous n'avez pas besoin d'obtenir une licence d'utilisation pour vous en servir.

L'utilisation d'un programme pare-feu personnalisé exige, dans les premiers temps, un investissement important de temps et d'effort. Vous devez vous assurer que tous les paramètres sont correctement réglés et adaptés à l'usage que vous faites de votre ordinateur. Une fois la période initiale d'apprentissage complétée, le pare-feu n'exigera que des interventions mineures de votre part.

**Avertissement!** N'accédez jamais à Internet si aucun pare-feu n'est installé sur votre ordinateur! Même si votre modem Internet ou votre routeur possèdent leur propre pare-feu, il est fortement recommandé que vous en installiez également un sur votre ordinateur.

#### Offline Installation Instructions :

##### Pour installer Comodo Firewall

- \*Lisez la courte **Introduction** aux **Guides pratiques** <sup>[1]</sup>\*\*
- **Cliquez sur l'icône Comodo Firewall ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- *Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.*
- *Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.*

Comodo Firewall:



[49]

## Comment installer Comodo Firewall

Sommaire des sections de cette page:

- [2.0 Survol du processus d'installation de COMODO Firewall](#)
- [2.1 Comment désactiver le pare-feu Windows](#)
- [2.2 Comment installer COMODO Firewall](#)

---

## 2.0 Survol du processus d'installation de COMODO Firewall

L'installation de **COMODO Firewall** est relativement simple et rapide. Elle comporte deux étapes: il faut dans un premier temps désactiver manuellement le pare-feu de Windows, et ensuite installer le logiciel **COMODO Firewall**.

Idéalement, vous ne devriez utiliser qu'un seul logiciel pare-feu sur votre ordinateur, en tout temps. Si vous utilisez actuellement un autre pare-feu sur votre ordinateur, vous devez le désinstaller avant d'installer **Comodo Firewall**, afin d'éviter les conflits possibles entre logiciels d'un même type.

### 2.1 Comment désactiver le pare-feu Windows

Pour désactiver le programme **Pare-feu Windows**, suivez les étapes énumérées ci-dessous:

**Première étape:** Sélectionnez Démarrer > Panneau de configuration > Pare-feu Windows pour afficher la fenêtre **\*\*Pare-feu Windows\*\***.

**Deuxième étape.** Cochez l'option *Désactivé (non recommandé)* pour désactiver le **Pare-feu Windows** tel qu'illustré ci-dessous:

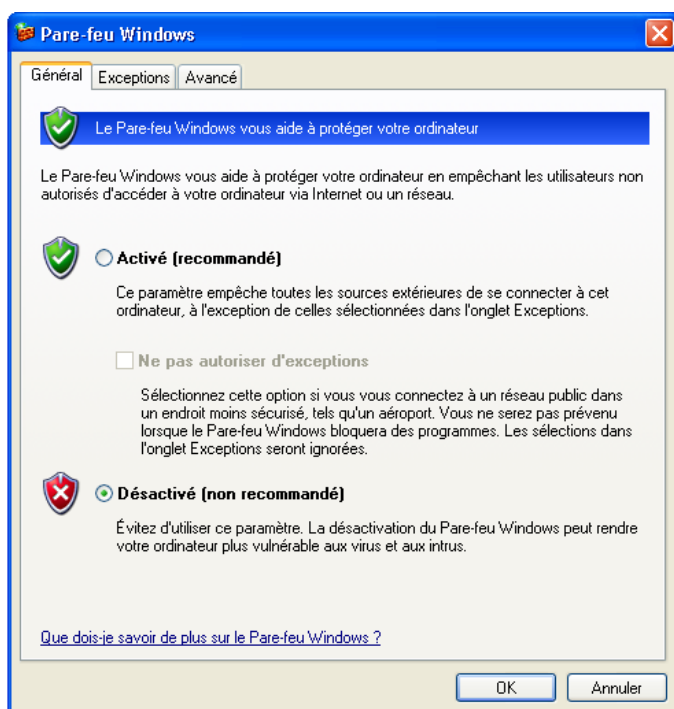



Figure 1. Le Pare-feu Windows avec l'option 'Désactivé' sélectionnée

Troisième étape. Cliquez sur  pour finaliser la désactivation du Pare-feu Windows.

## 2.2 Comment installer COMODO Firewall

**Commentaire:** COMODO Firewall ne désinstalle pas automatiquement les versions plus anciennes de son logiciel. Celles-ci doivent être désinstallées manuellement avant d'entamer le processus d'installation de la plus récente version.

Pour lancer l'installation de **COMODO Firewall**, suivez les étapes énumérées ci-dessous:

**Première étape.** Double-cliquez sur  cfw\_installer\_x86 pour entamer le processus d'installation. Si une boîte de dialogue *Fichier ouvert - Avertissement de sécurité* s'affiche, cliquez sur  pour afficher la boîte de dialogue suivante:

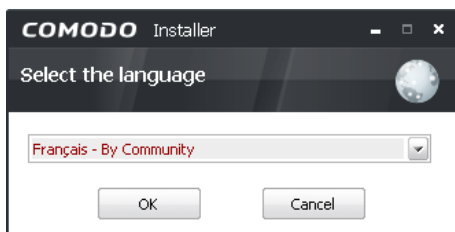


Figure 2: La boîte de dialogue de sélection de la langue

**Deuxième étape.** Cliquez sur  pour afficher le *Contrat de licence de l'utilisateur*. Veuillez lire attentivement le *Contrat de licence de l'utilisateur* avant de poursuivre le processus d'installation du logiciel, puis cliquez sur  pour afficher la fenêtre *Enregistrement gratuit*.

**Troisième étape:** **Ne saisissez pas** votre adresse email dans le champs *Entrez votre adresse email (facultatif)*; cliquez simplement sur  pour afficher la fenêtre d'extraction des fichiers.

Lorsque le processus d'extraction est complété, la fenêtre *Dossier de destination* s'affiche.

**Quatrième étape.** Cliquez sur  pour accepter l'emplacement par défaut et afficher la fenêtre *Sélection du niveau de sécurité du pare-feu*, puis **cochez** l'option *Pare-feu seulement*, tel qu'illustré ci-dessous:

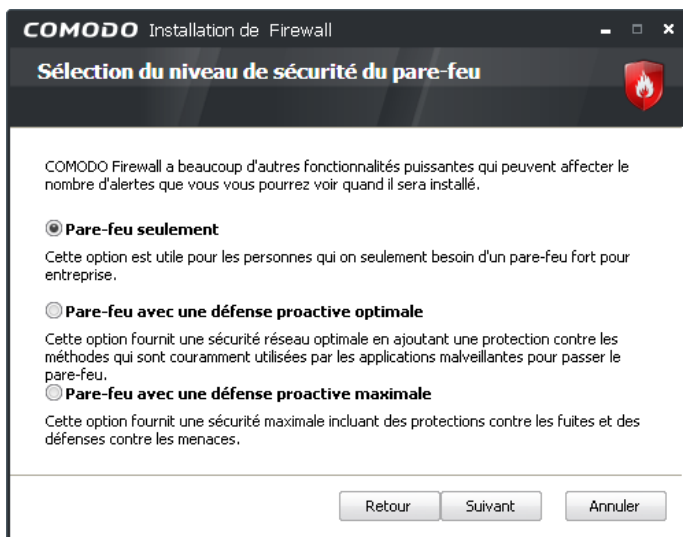


Figure 3: La fenêtre Sélection du niveau de sécurité du pare-feu

### Définition des différents niveau de sécurité du pare-feu

Chaque niveau de sécurité du pare-feu répond aux besoins particuliers d'utilisateurs de différents niveaux. Chaque option équilibre différents types de protection selon la complexité de l'utilisation et détermine le nombre d'avertissements de sécurité que vous pourriez recevoir. Voici une brève description de chaque niveau de sécurité:

**Le mode Pare-feu seulement:** Ce mode vous permet d'utiliser **COMODO Firewall** sans la fonction *Defense +*. Le logiciel identifie les applications les plus couramment utilisées et qui sont relativement sûres (comme les navigateurs Web et les clients de courrier électronique), ce qui réduit le nombre d'avertissements de sécurité que vous pourriez recevoir. Dans ce mode, le programme explique en termes généraux pourquoi un avertissement en particulier s'affiche dans telle ou telle circonstance. De plus, les actions à entreprendre sont relativement simples.

**Le mode Pare-feu avec une défense proactive optimale:** Ce mode ajoute la fonction *Defense +* à la bonne protection de base du mode **Pare-feu seulement**. *Defense +* offre une protection active contre les logiciels malveillants conçus spécifiquement pour contourner différents pare-feu. Les *Avertissements Comodo Firewall* présentent des explications approfondies des raisons pour lesquelles certaines applications ou requêtes sont bloquées, et vous donnent l'option d'isoler des fichiers ou programmes suspects ou de les placer dans une 'sandbox'.

**Le mode Pare-feu avec une défense proactive maximale:** Ce mode combine l'option **Pare-feu avec une défense proactive optimale** avec une fonction de protection 'anti-fuite' contre les menaces 'passives', par exemple lorsque des renseignements concernant les ports ouverts sur votre ordinateur sont envoyés sur Internet. La fonction 'sandbox' est complètement automatique.

**Sixième étape.** Cliquez sur  pour afficher la fenêtre *Configuration de COMODO Secure DNS*, avec l'option *Je veux utiliser les serveurs COMODO SecureDNS* sélectionnée, tel qu'illustré ci-dessous:

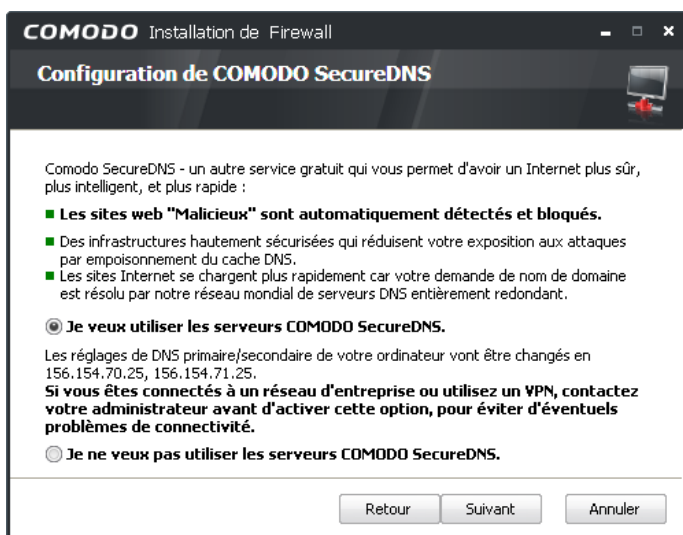


Figure 4: La fenêtre Configuration de COMODO Secure DNS

**Important:** Même si aucun **Système de noms de domaine (DNS)** n'est parfaitement sécurisé les bénéfices liés à l'utilisation des **\*\* Serveurs COMODO Secure DNS\*\*** sont plus nombreux que les inconvénients. Cette fonction vous offre une protection supplémentaire contre le *dévoisement (pharming)* et l'*hameçonnage (phishing)*, deux techniques de piratage courantes employées par des tiers malveillants pour détourner votre ordinateur vers des sites hostiles ou dangereux. Facile à configurer à l'installation, la fonction **serveurs COMODO Secure DNS** peut également vous protéger des interférences du gouvernement et facilite l'accès sécurisé aux sites Internet qui sont inscrits auprès de **COMODO**. Par exemple, si vous faites une faute en saisissant une URL, vous recevrez un avertissement du **Serveur COMODO Secure DNS** semblable à celui-ci:

Sorry, "www.www.gmail.com" does not exist or could not be found

The website you are looking for may be experiencing problems, is temporarily unavailable, or there was a typing error in the address. Error: (DNS), click the [back](#) button to try another link.

Figure 5: Un exemple typique d'avertissement du Serveur COMODO Secure DNS

**Septième étape.** Cliquez sur  pour afficher la fenêtre *Prêt à installer COMODO Firewall*, puis cliquez sur  pour lancer l'installation et afficher la fenêtre

*Installation de COMODO Firewall en cours.* À l'issue du processus d'installation, la fenêtre *L'installation du COMODO Firewall est terminée* s'affiche.

**Huitième étape.** Cliquez sur  pour afficher la fenêtre de confirmation *Fait*, puis cliquez à nouveau sur  pour afficher la fenêtre de confirmation illustrée ci-dessous:

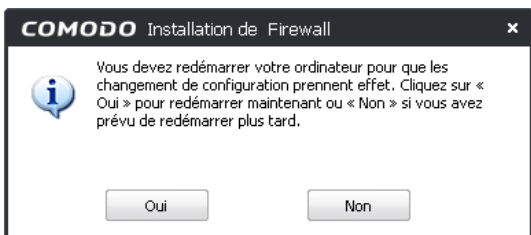


Figure 6: La fenêtre de confirmation *Installation de Firewall*

**Neuvième étape.** Cliquez sur  pour redémarrer l'ordinateur et finaliser la procédure d'installation de **COMODO Firewall**.

Après avoir redémarré votre ordinateur, la fenêtre *Nouveau réseau privé détecté* s'affiche comme suit:

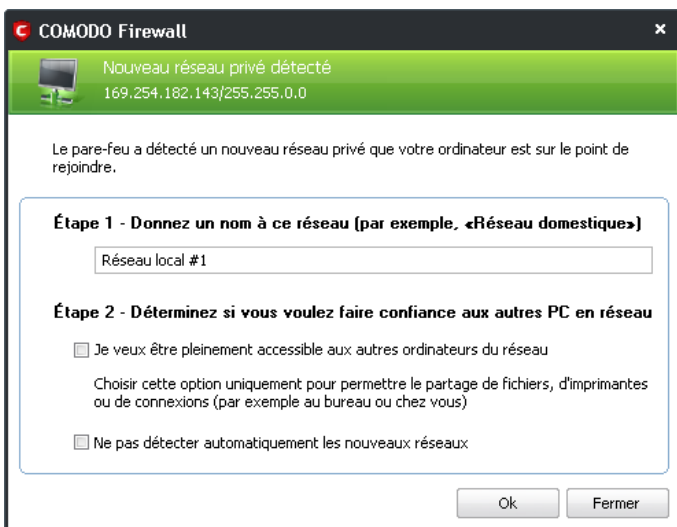


Figure 7: La fenêtre *Nouveau réseau privé détecté* de **COMODO Firewall**

**Astuce:** Si vous travaillez dans un environnement LAN, cochez l'option *Je veux être pleinement accessible aux autres ordinateurs du réseau* pour activer les fonctions de partage de fichiers/dossiers/imprimantes et/ou de connexion à Internet.

**Dixième étape.** Dans le champs *Donnez un nom à ce réseau*, saisissez un nouveau nom ou acceptez le nom par défaut tel qu'illustré à la Figure 7 ci-dessus. Laissez les options de la rubrique *Étape 2 - Déterminez si vous voulez faire confiance aux autres PC en réseau* désélectionnées, puis cliquez sur  pour finaliser l'installation.

L'icône de bureau **COMODO Firewall** et l'icône de connectivité **COMODO Firewall** apparaissent en même temps que la fenêtre illustrée à la figure 7. Avant de vous connecter à Internet, l'icône de connectivité s'affiche dans la barre des tâches, tel qu'illustré ci-dessous:



Figure 8: L'icône de connectivité de **COMODO Firewall** (ici surligné en noir) dans la barre des tâches

Lorsque une requête est faite pour aller sur Internet ou lancer un programme qui doit accéder à Internet (par exemple, un navigateur Web), une série de flèches orange pointant vers le bas et de flèches verte pointant vers le haut s'afficheront pour indiquer toute requête de connexion entrante ou sortante à Internet, tel qu'illustré ci-dessous:



Figure 9: L'icone de connectivité de COMODO Firewall en action

Après quelques minutes de fonctionnement, le Centre de messagerie de COMODO affichera peut-être un message comme celui-ci:

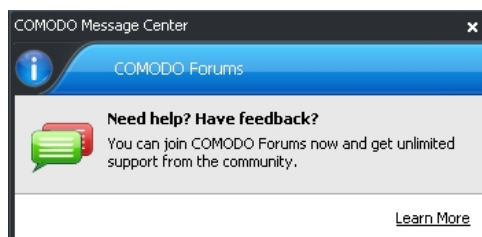


Figure 10: La fenêtre du Centre de messagerie de COMODO

**Commentaire:** Cliquez sur le lien *Learn more* pour être automatiquement redirigé vers les forums d'aide de **Comodo**.

**Astuce:** Cliquez à droite sur l'icone de connectivité de **COMODO Firewall** dans la *Barre des tâches* (tel qu'illustré à la figure 10) pour afficher le menu contextuel suivant, ainsi que ses sous-menus:

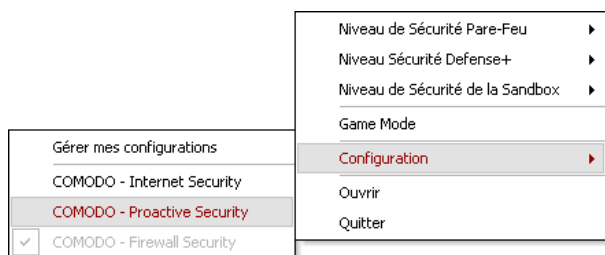


Figure 11: Le menu et les sous-menus contextuels de l'icone de connectivité

Le menu de l'icone de connectivité vous permet de changer les produits de **COMODO Firewall** que vous utilisez. En **sélectionnant** l'item *Configuration*, vous activez le sous-menu *Gérer mes configurations*, où vous pouvez **sélectionner** soit *COMODO - Proactive Security*, soit *COMODO - Internet Security* afin d'activer la fonction 'Sandbox'.

De plus, il est possible d'ajuster le niveau de sécurité de chaque produit à partir du menu contextuel de l'icone de connectivité, tel qu'illustré ci-dessous; ces niveaux de sécurité sont examinés plus attentivement dans les sections **4.1 La fenêtre de réglages du comportement du pare-feu** et **4.2 La fenêtre de réglages de Defense+**

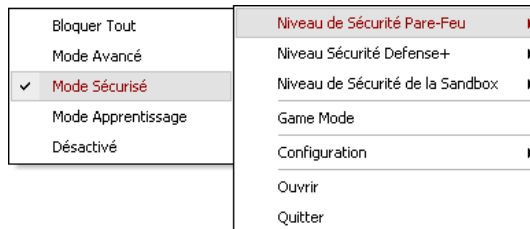


Figure 12: Le sous-menu 'Niveau de sécurité Pare-feu' de l'icone de connectivité

## Comment utiliser COMODO Firewall

Sommaire des sections de cette page:

- **[3.0 Comment autoriser ou bloquer des accès avec COMODO Firewall](#)**
- **[3.1 Comment ouvrir l'interface principale de COMODO Firewall](#)**
- **[3.2 Un survol de l'interface principale de COMODO Firewall](#)**

---

### 3.0 Comment autoriser ou bloquer des accès avec COMODO Firewall

Un pare-feu est un programme conçu pour protéger votre ordinateur contre des pirates ou des logiciels malveillants. Ces derniers peuvent tenter d'accéder directement à votre ordinateur ou d'envoyer des données à partir de votre ordinateur vers une tierce partie. **Comodo Firewall** doit être configuré correctement pour lui permettre d'apprendre et d'enregistrer quelles sont les applications qui sont "sûres" afin de leur autoriser l'accès, et de bloquer les requêtes provenant de logiciels dangereux et/ou constituent des menaces.

Chaque fois que **Comodo Firewall** reçoit une requête de connexion, il affiche une fenêtre *Alerte Pare-feu* vous demandant d'*autoriser* ou de *bloquer* l'accès de votre système depuis ou vers l'Internet. L'exercice qui suit concerne un programme sûr (**Firefox**) et vous aidera à vous familiariser avec les alertes pare-feu et à les utiliser correctement. Même si des exceptions sont parfois faites pour les requêtes provenant de navigateurs et clients de courrier électronique universellement reconnus, chaque fois qu'une requête de connexion est faite, une *Alerte pare-feu* semblable à celle-ci s'affiche:



Figure 1: Un exemple d'alerte pare-feu de COMODO

Un pare-feu n'est rien d'autre qu'un ensemble de règles servant à contrôler le trafic entrant et sortant. Chaque fois que vous cliquez sur *Autoriser* ou *Bloquer*, **COMODO Firewall** génère une règle sur mesure pour la requête au réseau de ce processus ou de ce programme. **COMODO Firewall** fait cela pour les processus et programmes nouveaux ou inconnus, ainsi que pour ceux compris dans la liste *Éditeurs de logiciels certifiés* de la fenêtre *Defense+ - Tâches > Stratégie de Sécurité*.

**Se souvenir de ma réponse:** Cette option est employée pour enregistrer si autorisez ou bloquez un programme en particulier. **COMODO Firewall**\* autorisera ou bloquera automatiquement les requêtes provenant de ce programme la prochaine fois qu'il tentera de se connecter, selon le choix que vous aurez fait préalablement.

**Important:** Nous recommandons fortement de désactiver la fonction *Se souvenir de ma réponse* lorsque vous commencez à utiliser **COMODO Firewall**. Décidez si vous autorisez ou bloquez différentes requêtes et observez quels effets vos décisions ont sur le fonctionnement de votre système. Activez la fonction *Se souvenir de ma réponse* si et *seulement si* vous êtes complètement sûr de votre décision.

**Astuce:** Limiter strictement l'accès à votre système est la meilleure façon d'en assurer la sécurité. N'hésitez pas à bloquer toutes les requêtes suspectes ou non identifiées. Si un blocage fait en sorte qu'un programme ne fonctionne plus normalement, vous pourrez autoriser la requête la prochaine fois que vous recevez une alerte du pare-feu.

**Première étape.** Cliquez sur *Application : firefox.exe* pour afficher la fenêtre *Propriétés* et obtenir des renseignements sur le processus ou le programme qui lance une requête, dans ce cas-ci, **Firefox**:

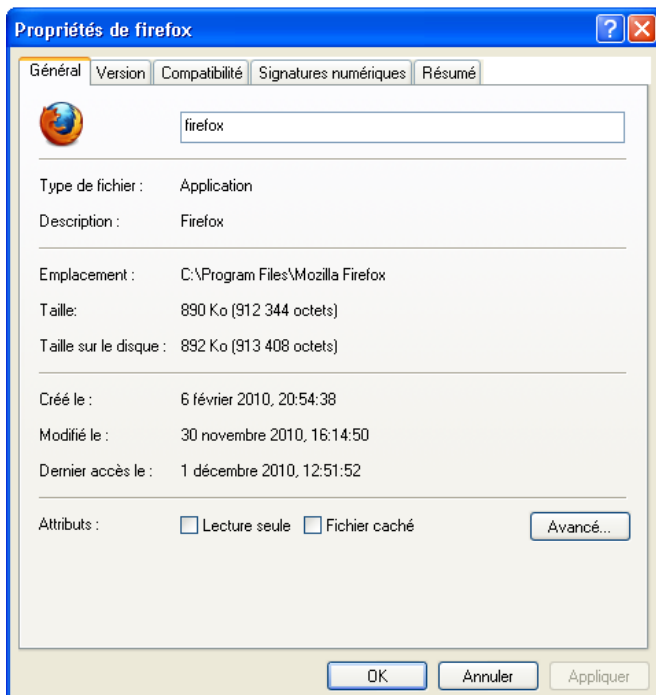




Figure 2: La fenêtre Propriétés de Firefox.exe

**Deuxième étape:** Cliquez sur  pour fermer la fenêtre *Propriétés* du programme.


**Troisième étape:** Selon les renseignements affichés dans la fenêtre *Propriétés*: si vous avez déterminé qu'une requête n'est pas sûre, ou si vous êtes incertain, cliquez sur  pour donner à **COMODO Firewall** la consigne de bloquer l'accès à votre système. OU: Si vous avez déterminé qu'un programme légitime lance une requête non malveillante,

cliquez sur  pour autoriser l'accès à votre système.

**Quatrième étape.** Cliquez sur  pour permettre à **Firefox** d'accéder à votre système par l'intermédiaire de **COMODO Firewall**.

**Cinquième étape.** Puisque **Firefox** est un programme considéré sûr, **cochez** l'option *Se souvenir de ma réponse* pour que **COMODO Firewall** autorise automatiquement l'accès à **Firefox** la prochaine fois et subséquemment.

**Commentaire:** Le bouton *Autoriser* vous permet d'autoriser manuellement, au cas par cas, l'accès à un processus ou un programme.

**Astuce:** Cliquez sur  *Que dois-je faire ?* pour accéder aux fiches d'aide en ligne de **COMODO Firewall**.

Votre capacité à prendre les bonnes décisions s'améliorera au fur et à mesure que vous prendrez de l'expérience avec **COMODO Firewall**.

### 3.1 Comment ouvrir l'interface principale de COMODO Firewall

**COMODO Firewall** démarrera automatiquement lorsque vous aurez installé le programme et redémarré votre système. Le programme comporte un panneau de configuration complet, avec de nombreuses fonctions et options flexibles. Les utilisateurs **débutants** apprendront facilement à gérer les alertes de sécurité **COMODO Firewall**, alors que les utilisateurs *expérimentés* et *avancés* pourront se familiariser avec des aspects plus complexes de la gestion et de la configuration du pare-feu.

**Commentaire:** Tous les exemples illustrés ici sont basés sur le mode *Défense optimale*. Cela signifie que le système de prévention des intrusions est activé automatiquement. Si vous avez installé **COMODO Firewall** avec l'option *Pare-feu seulement, Defense+* ne sera pas activé.

Pour ouvrir l'interface principale de **COMODO Firewall** suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez **Démarrer > Programmes > Comodo > Firewall > Comodo Firewall**.

**Commentaire:** Vous pouvez également afficher l'interface principale du programme en **double-cliquant** sur l'icône de bureau, ou en **double-cliquant** sur l'icône **COMODO Firewall** qui se trouve dans la *Barre des tâches*. De plus, vous pouvez **cliquer à droite** sur l'icône **COMODO Firewall** pour afficher le menu contextuel, puis **sélectionner ouvrir**, comme suit:

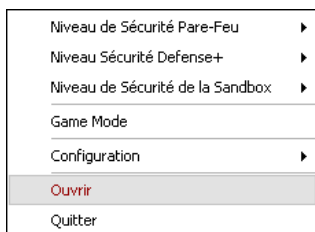


Figure 3: Le menu contextuel à partir de l'icône de connectivité COMODO Firewall




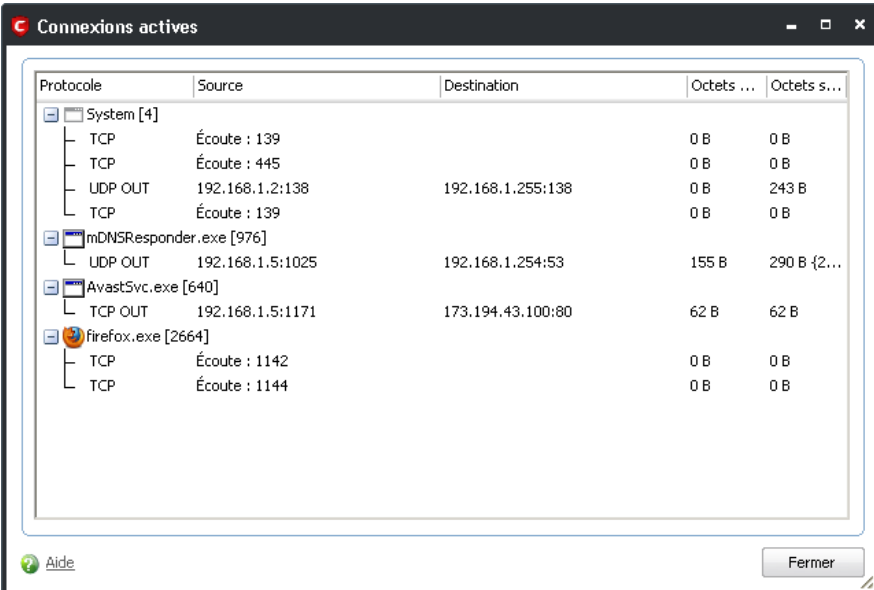
Figure 4: L'interface principale de Comodo Firewall, en mode Sommaire par défaut



## 3.2 Un survol de l'interface principale de COMODO Firewall


La fenêtre *Pare-feu* affiche un sommaire clair et concis des requêtes entrantes et sortantes des processus et programmes qui tentent de se connecter par l'entremise de **COMODO Firewall**. Il y a habituellement davantage de requêtes sortantes que de requêtes entrantes. Le mode de fonctionnement par défaut est le *Mode sécurisé*. Les différents modes seront abordés plus loin dans cette section. Le *Trafic* affiche les différents processus et programmes en cours et le nombre de requêtes effectuées, sous forme de pourcentage.



Cliquez sur  33 connexion(s) sortante(s) pour afficher les sommaires détaillés des requêtes sortantes *en tout temps*, comme suit:





Protocole	Source	Destination	Octets ...	Octets s...
System [4]				
TCP	Écoute : 139		0 B	0 B
TCP	Écoute : 445		0 B	0 B
UDP OUT	192.168.1.2:138	192.168.1.255:138	0 B	243 B
TCP	Écoute : 139		0 B	0 B
mDNSResponder.exe [976]				
UDP OUT	192.168.1.5:1025	192.168.1.254:53	155 B	290 B {2...
AvastSvc.exe [640]				
TCP OUT	192.168.1.5:1171	173.194.43.100:80	62 B	62 B
Firefox.exe [2664]				
TCP	Écoute : 1142		0 B	0 B
TCP	Écoute : 1144		0 B	0 B

Figure 5: Un exemple de fenêtre de Connexions actives affichant les détails du trafic Internet

Cliquez sur  1 connexion(s) entrante(s) pour afficher la fenêtre des *Connexions actives* des requêtes entrantes, *en tout temps*.

**Astuce:** Cliquez sur  **Stopper Tout Trafic** pour arrêter toutes les requêtes entrantes et sortantes, si votre service Internet ralentit ou plante soudainement, et/ou si vous avez des raisons de croire qu'un processus ou un programme malveillant est en cours de téléchargement ou d'opération. Ce faisant, vous mettez automatiquement le *pare-feu* en mode de fonctionnement  **Bloquer Tout**. Réviser le sommaire détaillé dans la fenêtre *Connexions actives* pour trouver les possibles sources du problème.

Après vous être assuré d'avoir résolu les problèmes, cliquez sur  **Ré-autoriser Tout Trafic** pour indiquer à **COMODO Firewall** de recommencer à traiter les requêtes entrantes et sortantes et retourner au  **Mode sécurisé** comme d'habitude.

### 3.2.1 Les icônes d'état de COMODO Firewall

**COMODO Firewall** et **Defense+** fonctionnent main dans la main; si les deux programmes sont en cours d'opération, l'icône qui se trouve à la gauche de l'interface principale s'affiche comme suit:

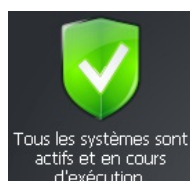


Figure 6: L'icône d'état vert de COMODO Firewall

Si l'un ou l'autre des programmes est désactivé, l'icône d'état indique que le pare-feu ou une des composants de la protection proactive est désactivé:

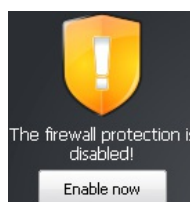



Figure 7: L'icône d'état jaune indiquant que le pare-feu est désactivé

Si les deux programmes sont désactivés, l'icône d'état s'affiche comme suit:

□

Figure 8: L'icone d'état jaune de COMODO Firewall indiquant que plusieurs protections sont désactivées

Dans un cas comme dans l'autre, **cliquez** sur  pour activer la protection correspondante.

## Configuration et paramètres avancés

Sommaire des sections de cette page:

- **4.0 Comment accéder aux fenêtres Pare-feu et Defense+**
- **4.1 La fenêtre Paramètres du comportement du Pare-feu**
- **4.2 La fenêtre Paramètres Defense+**

### 4.0 Comment accéder aux fenêtres Pare-feu et Defense+

L'interface principale de **COMODO Firewall** est séparée en deux panneaux, le panneau *Pare-feu* et le panneau *Defense+*.

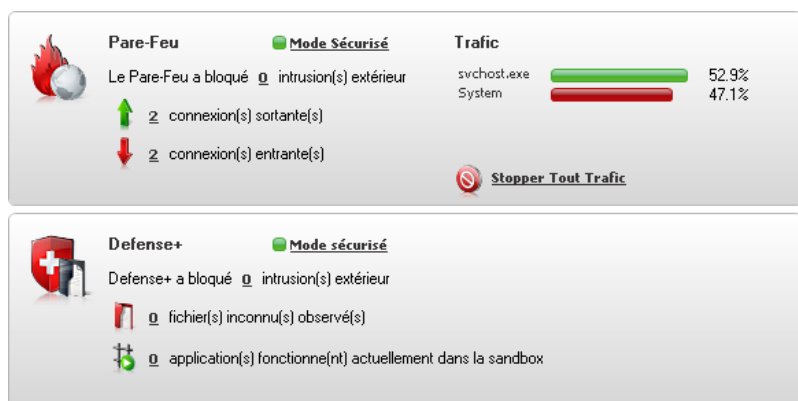



Figure 1: L'interface principale de COMODO Firewall affichant les panneaux Pare-feu et Defense+

On accède aux fenêtres *Paramètres du comportement du Pare-feu* et *Paramètres Defense+* en **cliquant** sur  dans l'un ou l'autre des panneaux pour afficher la fenêtre correspondante et les onglets associés.

On peut également accéder à l'une ou l'autre de ces fenêtres en suivant les étapes énumérées ci-dessous:

**Première étape. Ouvrez** l'interface principale de **COMODO Firewall**.

**Deuxième étape. Cliquez** sur



pour afficher la fenêtre *Tâches du Pare-feu* ou *Tâches Defense+*, respectivement.

**Troisième étape. Cliquez** sur



Pour afficher le contenu de l'onglet *Paramètres du comportement du pare-feu* OU celui de l'onglet *Paramètres Defense+*, respectivement.

**Astuce:** Les *Niveau de Sécurité Pare-feu*, *Niveau de Sécurité Defense+* et *Niveau de Sécurité de la Sandbox*, qui sont abordés dans la prochaine section, peuvent être réglés facilement et efficacement en passant par l'icone de connectivité de **COMODO Firewall** qui se trouve dans la *Barre des tâches Windows*. **Cliquez à droite** sur l'icone de connectivité pour afficher le menu contextuel et les sous-menus, tel qu'illustré ci-dessous:

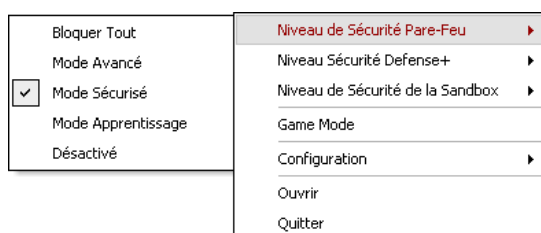


Figure 2: Le menu contextuel de l'icone de connectivité affichant le niveau de sécurité du Pare-feu

### 4.1 La fenêtre des paramètres du comportement du Pare-feu

La fenêtre **\*\*Paramètres du comportement du Pare-feu** vous permet de personnaliser le pare-feu avec une panoplie d'options et de fonctionnalités, dont le niveau de sécurité du pare-feu, la fréquence et le type d'alertes à recevoir, ainsi que

l'analyse et la surveillance des paquets.

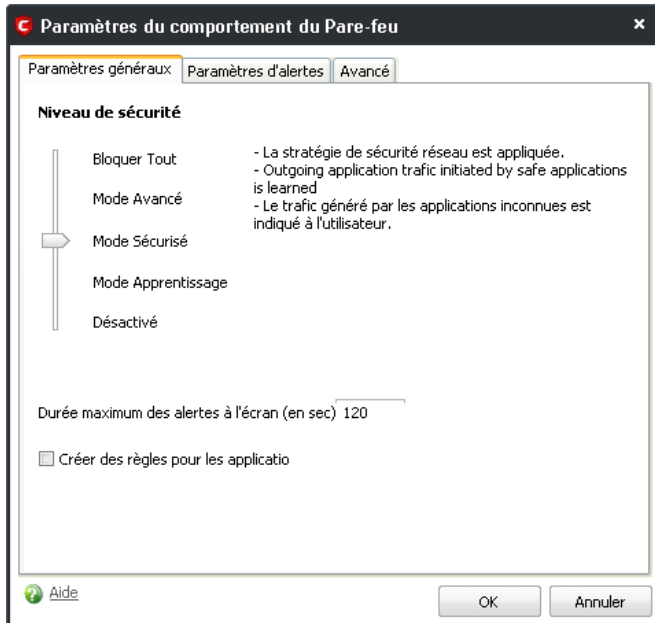


Figure 3: La fenêtre Paramètres du comportement du pare-feu - Paramètres généraux

L'onglet *Paramètres généraux* vous permet de spécifier le niveau de sécurité que vous jugez approprié pour **COMODO Firewall**. Le glisseur vous permet de choisir parmi les niveaux de sécurité suivants: toutes **Bloquez tout**: Ce mode bloque tout le trafic Internet et outrepassé tous les réglages et toutes les règles que vous avez déterminées. Ce mode ne génère aucune règle de trafic pour les applications et n'enregistre pas leur comportement.

**Mode avancé**: Ce mode applique *uniquement* les stratégies de sécurité et de réseautage déterminées par l'utilisateur dans les fenêtres *Tâches Pare-feu > Stratégie de Sécurité Réseau* et *Tâches Dedense+ > Stratégie de Sécurité*.

**Mode sécurisé**: Ce mode est le réglage par défaut de **COMODO Firewall**, y compris les installations *Défense proactive optimale* et *Défense proactive maximale*.

**Astuce**: **COMODO Firewall** maintient une liste interne des applications et fichiers régulièrement utilisés qui ont été définis comme sûrs, et n'émet pas d'alertes pour ceux-ci.

**Avertissement**: Les modes *Apprentissage* et *Désactivé* ne sont pas recommandés car ils peuvent nuire à l'efficacité de **COMODO Firewall** et exposer votre ordinateur à des risques d'infection.

## 4.2 La fenêtre Paramètres Defense+

**Commentaire**: Les fonctionnalités et options décrites dans cette section exigent une compréhension approfondie des pare-feu et des questions de sécurité, et est par conséquent principalement conçu pour les utilisateurs de niveau *avancé*.

**Important**: si vous avez coché l'une ou l'autre des options **Pare-feu avec défense proactive optimale\*** et **Pare-feu avec défense proactive maximale** lors du processus d'installation de **COMODO Firewall**, le système de prévention des intrusions *Defense+* a été automatiquement activé. Cela dit, si vous avez coché l'option *Pare-feu seulement*, le système *Defense+* peut tout de même être activé manuellement. L'option *Defense+* doit être activée pour que plusieurs des fonctionnalités décrites ci-dessous soient en mesure de fonctionner.

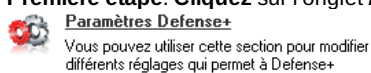
La fonction *Defense+* de **COMODO Firewall** est un système de prévention des intrusions. Tout ordinateur connecté à un réseau est techniquement un ordinateur hôte. Le système *Defense+* surveille continuellement les activités de tous les fichiers exécutables qui se trouvent actuellement sur votre ordinateur. Un fichier exécutable est une application ou un programme, ou une partie d'un programme, est habituellement (mais pas nécessairement) identifiable par l'un ou l'autre des extensions de fichiers suivants: *.bat*, *.exe*, *.dll*, *.sys*, ou d'autres.

*Defense+* émet des alertes chaque fois qu'un fichier exécutable inconnu tente de s'exécuter, et vous demande d'autoriser ou de bloquer son exécution. Ce système peut s'avérer important dans les situations où des logiciels malveillants essaieraient d'installer des applications ou des programmes pour endommager ou voler vos données personnelles, reformater votre disque dur ou détourner votre système pour propager des programmes malveillants ou du pourriel sans votre consentement ou votre connaissance.

### 4.2.1 La fenêtre Paramètres Defense+ - Onglet Paramètres généraux

Pour activer manuellement le système *Defense+* et afficher la fenêtre *Paramètres Defense+*, suivez les étapes énumérées ci-dessous:

**Première étape**. Cliquez sur l'onglet *Defense+* dans l'interface principale de **COMODO Firewall**, puis cliquez sur



pour afficher la fenêtre suivante:

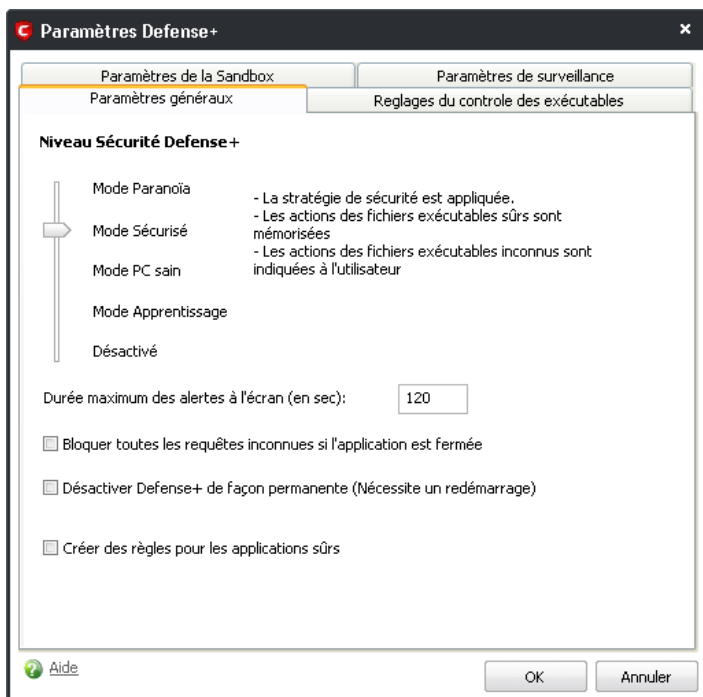


Figure 6: La fenêtre Defense+ affichant l'onglet Paramètres général par défaut

**Deuxième étape.** Faites passer le glisseur au *Mode sécurisé*, puis **cliquez** sur  pour activer le système Defense+ tel qu'illustré à la Figure 6.

Le *Niveau de Sécurité Defense+* ressemble au *Niveau de sécurité du comportement du Pare-feu*, offre des options similaires, et vous permet d'utiliser le glisseur pour choisir le niveau de protection optimal contre les intrusions.

**Mode Paranoïa:** Ce mode offre le niveau de sécurité le plus élevé; il comprend une surveillance automatique de tous les fichiers exécutables, à part ceux que vous avez définis comme sûrs, y compris ceux inclus dans la liste des *Éditeurs de logiciels certifiés*. Ce mode comporte la plus haute fréquence d'alertes de sécurité, et l'activité du système est filtrée à travers les paramètres de votre configuration.

**Mode sécurisé:** Ce mode 'apprend' automatiquement les comportements des différentes applications exécutables, tout en surveillant les activités critiques du système. Toutes les applications non certifiées génèrent une *Alerte de sécurité* chaque fois qu'elles sont mises en exécution. Ce mode est le plus recommandé pour la majorité des utilisateurs.

- L'option *Bloquer toutes les requêtes inconnues si l'application est fermée* bloque automatiquement toutes les requêtes émises par des applications et des programmes inconnus, ou que vous n'avez pas spécifié dans votre *Stratégie de sécurité*.
- L'option *Désactiver Defense+ de façon permanente (nécessite un redémarrage)* vous permet de désactiver manuellement le système de prévention des intrusions \* Defense+. Cette option n'est généralement pas recommandée.

#### 4.2.2 Les paramètres Defense+ - Onglet Réglages du contrôle des exécutable

L'onglet *Réglages du contrôle des exécutable* limite l'auto-exécution des fichiers suspects ou inconnus (ainsi que leur accès aux ressources de votre ordinateur), et soumet ceux-ci à une analyse.

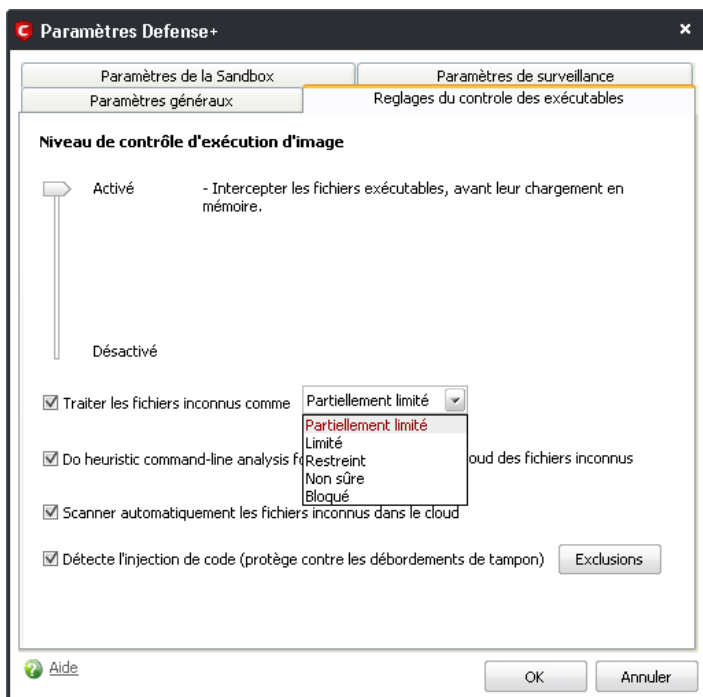



Figure 7: L'onglet Réglages du contrôle des exécutable

**Astuce:** Les utilisateurs de niveau **avancé** peuvent créer des exclusions aux tâches susmentionnées en cliquant sur  pour afficher le panneau *Exclusions* et sélectionner différents processus et programmes à exclure.

**Commentaire:** Les utilisateurs de niveau **expérimenté** et **avancé** sont fortement encouragés à **cliquer** sur  *Aide* pour accéder aux fiches d'aide en ligne de **COMODO** qui concernent les onglets *Réglages du contrôle des exécutable*, les *Paramètres de la Sandbox* et les *Paramètres de surveillance*. Vous pouvez également vous référer à <http://help.comodo.com/topic-72-1-155-1074-Introduction-to-Comodo-Internet-Security.html> pour choisir une fiche à partir d'une liste de rubriques d'aides en ligne.

## Faq et questions récapitulatives

### 5.0 Faq et questions récapitulatives

Muhindo et Salima sont agréablement surpris de constater à quel point **COMODO Firewall** est facile à utiliser et fonctionne silencieusement en arrière-plan. Il leur reste cependant quelques questions.

**Q:** Si je n'ai pas de pare-feu, peux-tu me parler davantage des menaces qui guettent mon ordinateur? Quels sont les différents types de programmes qui peuvent accéder à mon ordinateur, et que font-ils?

**A:** Il existe des milliers de programmes qui peuvent accéder à ton ordinateur depuis Internet s'il n'y a pas de pare-feu installé. Il existe même des "araignées" du Web (ou robots) qui parcourent toutes les adresses possibles à la recherche d'ordinateurs qui ne sont pas munis d'un pare-feu fonctionnel. Lorsqu'elles trouvent ces adresses, les araignées les rapportent aux pirates. De plus, il existe des programmes conçus pour 'détourner' ton ordinateur et l'utiliser pour mener des transactions illégales ou disséminer du pourriel sans ton consentement ou ta connaissance: tu pourrais potentiellement être accusé pour des activités illégales dont tu es complètement innocent!

**Q:** Si **COMODO Firewall** garde tous ces programmes à distance, pourquoi ai-je aussi besoin d'un programme antivirus et d'un programme anti-logiciel espion?

**A:** Un pare-feu se concentre sur la restriction de l'accès depuis et vers Internet. Il empêche un programme ou un pirate d'accéder à ton ordinateur, mais ne peut pas te protéger des logiciels malveillants qui sont téléchargés, par exemple, par messagerie électronique, depuis des sites Internet ou depuis des disques externes. **COMODO Firewall** comprend en outre **Defense+**, un système de prévention des intrusions qui surveille en permanence les types de fichiers exécutable autorisés à fonctionner sur notre système. Les programmes antivirus et anti-logiciel espion servent à empêcher la contamination là où le pare-feu est impuissant. De plus, ces outils peuvent également retirer des logiciels malveillants déjà installés sur ton ordinateur.

**Q:** Devrais-je être vigilant à l'égard de logiciels malveillants qui ont l'apparence de programmes Windows (ou d'autres programmes inoffensifs)?

**A:** Malheureusement, de nombreux programmes sont conçus ainsi. Tu dois être très vigilant quant à l'origine d'un programme lorsque tu le télécharges ou l'installes. Tu ne devrais installer aucun logiciel qui n'est pas absolument utile et nécessaire à ton travail, surtout sur des ordinateurs qui contiennent beaucoup de données importantes ou délicates. C'est à cet égard que le système de prévention des intrusions **COMODO Defense+** peut s'avérer fort utile; en comparant chaque nouvel exécutable des applications récemment installées avec une liste d'éditeurs de logiciels certifiés et en soumettant à l'analyse tout logiciel potentiellement malveillant, cet outil améliore considérablement ta sécurité sur Internet.

**Q:** Dans quelle mesure **COMODO Firewall** offre-t-il une protection efficace contre les pirates?

**A:** **COMODO Firewall** offre un contrôle complet et raffiné de l'accès à la plateforme \*Windows. Cela dit, un pare-feu n'est efficace que dans la mesure où sa configuration est appropriée. En dépit des inconvénients mineurs que présentent un pare-feu, il est fortement recommandé de persister dans son utilisation. Continue à t'informer sur **COMODO Firewall**; plus

tu sera familier avec le programme, plus tu comprendras à quel point la protection qu'il t'offre est avantageuse.\*

## 5.1 Questions récapitulatives

- Peut-on employer plus d'un pare-feu à la fois?
- Comment peut-on vérifier si un programme avec lequel on n'est pas familier est suffisamment sûr pour le laisser s'exécuter sur notre ordinateur?
- Comment le pare-feu fonctionne-t-il?
- Quelle est la différence entre un pare-feu et un système de prévention des intrusions?
- Pourquoi dois-je installer un pare-feu?

## KeePass - stockage de mots de passe

### Short Description:

**KeePass** est un outil de gestion de mots de passe sécurisé et facile à utiliser.

### Online Installation Instructions:

#### Pour télécharger KeePass

- Lisez la courte introduction aux **Guides pratiques** <sup>[1]</sup>
- Cliquez sur l'icône **KeePass** ci-dessous pour ouvrir la page de téléchargement [www.keepass.info/download.html](http://www.keepass.info/download.html)
- Dans la section "**Classic Edition**", cliquez sur "**KeePass 1.xx (Installer EXE for Windows)**".
- Sauvegardez le fichier d'installation **KeePass-1.xx-Setup.exe** à un emplacement de votre choix, puis cliquez dessus pour lancer l'installation.
- Vous pouvez supprimer l'exécutable après l'installation.

### Keepass:



<sup>[50]</sup>

#### Pour utiliser KeePass en français

- **Installez KeePass** en suivant les consignes indiquées à la section **2.0 Comment installer KeePass** <sup>[51]</sup>
- Rendez-vous à la **page web des traductions de KeePass** <sup>[52]</sup>
- Localisez le fichier .zip de traduction française **French-1.xx.zip** et sauvegardez-le sur votre ordinateur à un emplacement de votre choix.
- Décompactez le fichier .zip, et copiez le fichier *French.lng* dans le répertoire où **KeePass** est installé (habituellement C:/Program Files/KeePass).
- **Démarrez KeePass**, allez au menu *View > Change Language...* et **sélectionnez French**.
- Redémarrez KeePass.

### Site Internet

[www.keepass.info](http://www.keepass.info) <sup>[53]</sup>

### Configuration requise

- Compatible avec toutes les versions de Windows

### Version utilisée pour rédiger ce guide

- 1.18

### Licence

- Free/libre Open Source Software (FOSS)

### Lecture préalable

- Livret pratique Security in-a-box, chapitre **3. Créer et sauvegarder des mots de passe sûrs** <sup>[54]</sup>.

**Niveau:** 1 : Débutant, 2 : **Moyen**, 3 : Intermédiaire, 4 : Expérimenté, 5 : Avancé

**Temps d'apprentissage:** 15 minutes

### Ce que vous apportera l'utilisation de cet outil:

- La capacité de sauvegarder tous vos mots de passe dans une seule base données (une base de mots de passe) pratique et sécurisée.
- La capacité de créer et de stocker plusieurs mots de passe forts (complexes) sans pour autant devoir les mémoriser.

### Autres programmes compatibles avec GNU Linux, Mac OS et Microsoft Windows:

**KeePass** est également compatible avec **GNU Linux** et **Mac OS** (dans sa version **KeePassX** <sup>[55]</sup> version). Il existe aussi des versions de **KeePass** pour d'autres plateformes, comme **iPhone**, **BlackBerry**, **Android**, **PocketPC**, etc. Si vous préférez essayer d'autres programmes similaires, nous recommandons:

- **Password Safe** <sup>[56]</sup>, compatible avec **Microsoft Windows** et **GNU Linux**
- **1Password** <sup>[57]</sup> compatible avec **Mac OS**, **Microsoft Windows**, **iPhone** et **iPad**

### 1.1 À propos de cet outil

**KeePass** est un outil puissant et facile à utiliser qui vous permettra de stocker et de gérer vos mots de passe dans une base de données, ou base de mots de passe, hautement sécurisée. Il vous sera possible de charger la base de mots de passe et le programme **KeePass** sur une clé USB que vous pourrez transporter sur vous. La base de mots de passe est protégée par un mot de passe principal que vous créez vous-même. Ce mot de passe unique sert à chiffrer l'ensemble du contenu de la base de mots de passe. Vous pouvez stocker vos mots de passe existants avec **KeePass** ou vous servir du logiciel pour en générer de nouveaux. KeePass ne requiert aucune configuration préalable et ne comporte pas d'instructions d'installation particulières. Le logiciel peut être utilisé aussitôt que VOUS êtes prêts à le faire!

#### Offline Installation Instructions :

##### Pour installer KeePass

- \*Lisez la courte **Introduction** aux **Guides pratiques** <sup>[1]\*\*</sup>
- **Cliquez sur l'icône KeePass ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- **Lisez attentivement les 'Consignes d'installation'** dans la prochaine section avant de poursuivre l'installation.
- **Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.**

KeePass:



[58] FR [59]


## Comment utiliser KeePass

Sommaire des sections de cette page:

- **2.0 Comment installer KeePass**
- **2.1 Comment créer une nouvelles base de mots de passe**
- **2.2 Comment ajouter une entrée**
- **2.3 Comment éditer une entrée**
- **2.4 Comment générer des mots de passe aléatoirement**
- **2.5 Comment fermer, réduire ou restaurer KeePass**
- **2.6 Comment créer une copie de sauvegarde de la base de mots de passe**
- **2.7 Comment réinitialiser votre mot de passe principal**

---

## 2.0 Comment installer KeePass

**Première étape.** Double-cliquez sur  KeePass-1.18-Setup ; si la boîte de dialogue *Fichier ouvert - avertissement de sécurité* s'affiche, cliquez sur  pour afficher la fenêtre suivante:

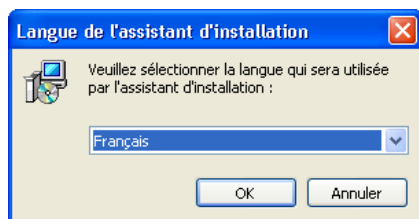


Figure 1: La fenêtre Langue de l'assistant d'installation

**Deuxième étape.** Cliquez sur  pour afficher la fenêtre *Installation - KeePass Password Safe – Bienvenue dans l'assistant d'installation de KeePass Password Safe*.

**Troisième étape.** Cliquez sur  pour afficher la fenêtre *Accord de licence*. Veuillez lire attentivement l'*Accord de licence* avant de poursuivre le processus d'installation.

**Quatrième étape.** Cochez l'option *Je comprends et j'accepte les termes du contrat de licence* pour activer le bouton *Suivant*, puis cliquez sur  pour afficher la fenêtre *Dossier de destination*.

**Cinquième étape.** Cliquez sur  pour accepter l'emplacement par défaut et afficher la fenêtre *Sélection du dossier du menu Démarrer*, puis cliquez sur  pour accepter le dossier par défaut.

**Sixième étape.** Cliquez sur  pour afficher la fenêtre suivante:

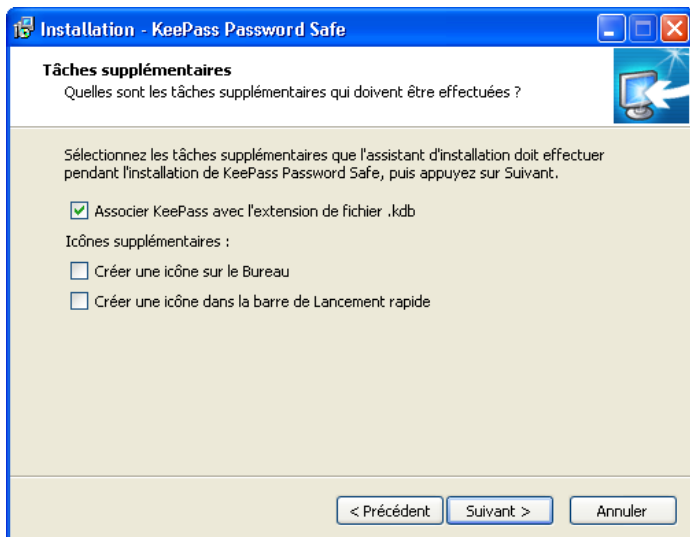


Figure 2: La fenêtre Tâches supplémentaires

**Septième étape.** Cochez l'option  Associer KeePass avec l'extension de fichier .kdb tel qu'illustré à la figure 2.

**Commentaire:** Si vous avez laissé l'option *Ne pas créer de dossier dans le menu Démarrer* désactivée à l'étape précédente, l'assistant d'installation de *KeePass Password Safe* crée automatiquement un icône de lancement rapide **KeePass** dans le menu *Démarrer*.

**Huitième étape.** Cliquez sur  pour afficher la fenêtre *Prêt à installer*, puis cliquez sur  pour afficher la fenêtre **Installation en cours** et sa barre de progression.


Quelques secondes plus tard, la fenêtre *Fin de l'installation de KeePass Password Safe* s'affiche.

**Neuvième étape.** Cochez l'option *Exécuter KeePass*, puis cliquez sur  pour ouvrir **KeePass** immédiatement, ainsi que la page web *Plugins and Extensions* de **KeePass** si vous êtes connecté à Internet.

## 2.1 Comment créer une nouvelles base de mots de passe

Dans les prochaines sections de ce guide, vous apprendrez à créer un mot de passe principal (clé maître), à sauvegarder la base de mots de passe nouvellement créée, à générer des mots de passe aléatoires pour un programme en particulier, à créer des copies de sauvegarde de votre base de mots de passe et à extraire les mots de passe de **KeePass** lorsque cela s'avère nécessaire.

Pour ouvrir **KeePass**, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez: **Démarrer > Programmes > KeePass Password Safe > KeePass** ou cliquez sur l'icône de bureau  pour afficher la fenêtre principale de **KeePass** illustrée ci-dessous :

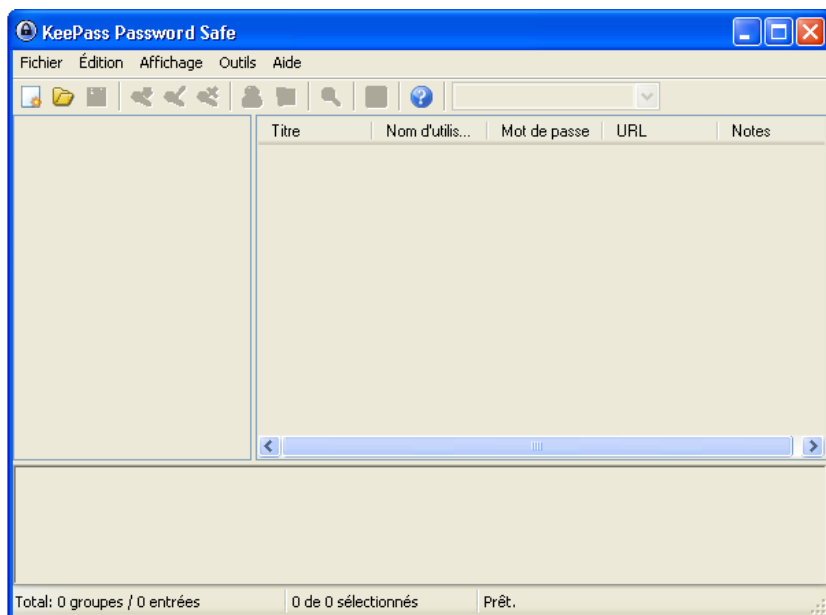


Figure 3: La console de KeePass Password Safe

### 2.1.1 Comment créer une nouvelles base de mots de passe

La création d'une nouvelle base de mots de passe comporte deux étapes: Vous devez inventer un mot de passe principal, fort (complexe) et unique, qui vous servira à verrouiller et déverrouiller votre banque de mots de passe. Vous devez



ensuite sauvegarder votre banque de mots de passe.

Pour créer une nouvelle base de mots de passe, suivez les étapes énumérées ci-dessous:

**Première étape. Sélectionnez: Fichier> Nouvelle**, comme suit:

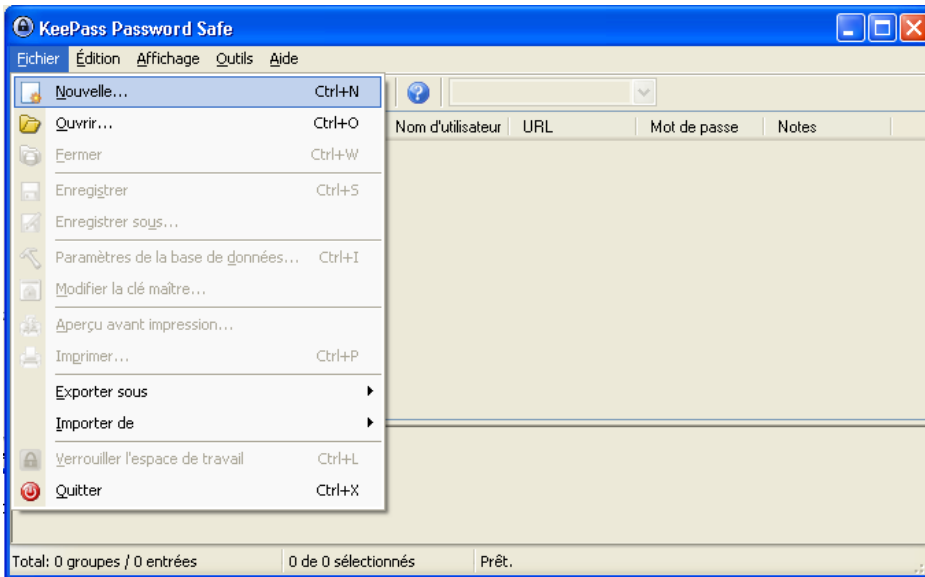


Figure 4: La fenêtre principale de KeePass, avec Fichier > Nouvelle sélectionné

Cela activera la fenêtre *Créer une Nouvelle base de Mots de Passe*, illustrée ci-dessous:

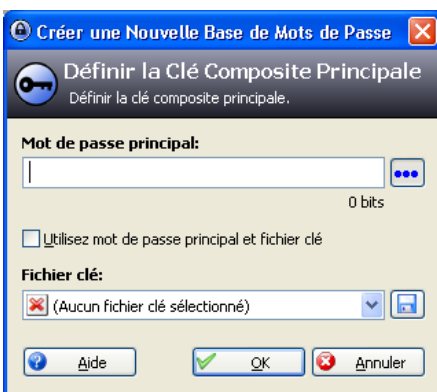


Figure 5: La fenêtre *Créer une Nouvelle base de Mots de Passe*

**Deuxième étape. Saisissez** le mot de passe maître que vous avez inventé dans la zone *Mot de passe principal*.

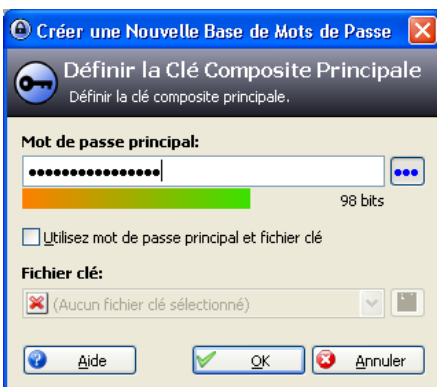
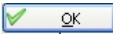


Figure 6: La fenêtre *Définir la Clé composite Principale*, avec la zone *Mot de passe principal* remplie

Vous verrez alors apparaître une barre de progression orange/vert sous la saisie du mot de passe. La barre passe du orange au vert au fur et à mesure que vous saisissez votre mot de passe, selon la complexité et la force du mot de passe choisi, et selon le nombre de caractères utilisés.

**Astuce:** Lorsque vous saisissez votre mot de passe, vous devriez essayer de faire en sorte qu'au moins la moitié de la barre soit colorée en vert.

**Troisième étape. Cliquez** sur  pour activer la fenêtre *Confirmer le Mot de passe principal* et confirmer votre mot de passe, comme suit:

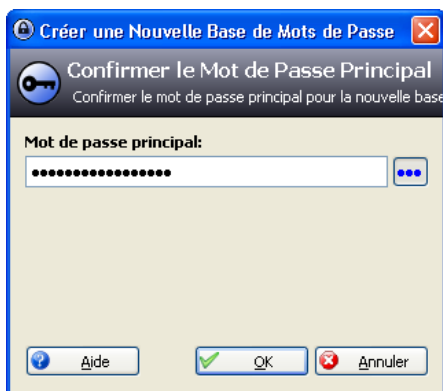
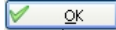



Figure 7: La fenêtre Confirmer le Mot de passe principal

**Quatrième étape.** Saisissez le même mot de passe qu'avant, puis **cliquez** sur 

**Cinquième étape.** Cliquez sur  pour voir si vous avez saisi votre mot de passe correctement.

**Attention:** Ceci n'est pas recommandé si vous craignez que quelqu'un vous espionne.

Lorsque vous aurez saisi deux fois votre mot de passe maître avec succès, la console principale de **KeePass** sera activée, tel qu'illustré ci-dessous :

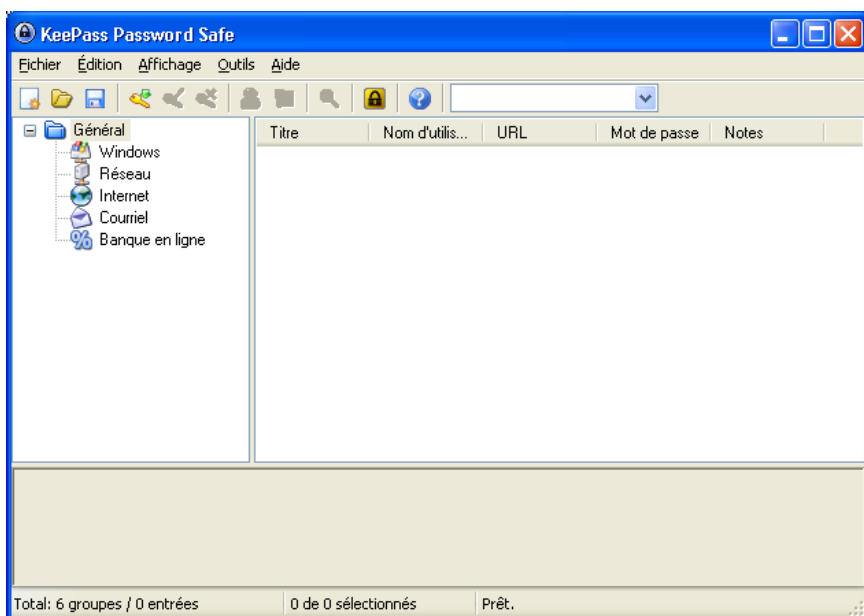


Figure 8: La fenêtre principale de KeePass Password Safe, en mode actif

Lorsque vous aurez créé la base de mots de passe, il vous faudra encore la sauvegarder. Pour sauvegarder la base de mots de passe, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez: **Fichier > Enregistrer sous:**

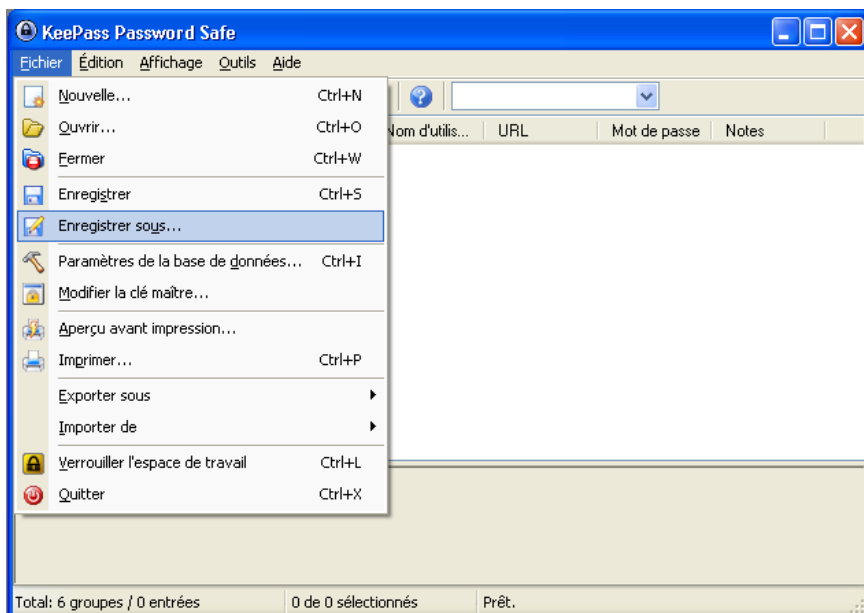


Figure 9: La fenêtre principale de KeePass, avec Fichier > Enregistrez sous sélectionné

Cela activera la fenêtre Enregistrez sous, illustrée ci-dessous:

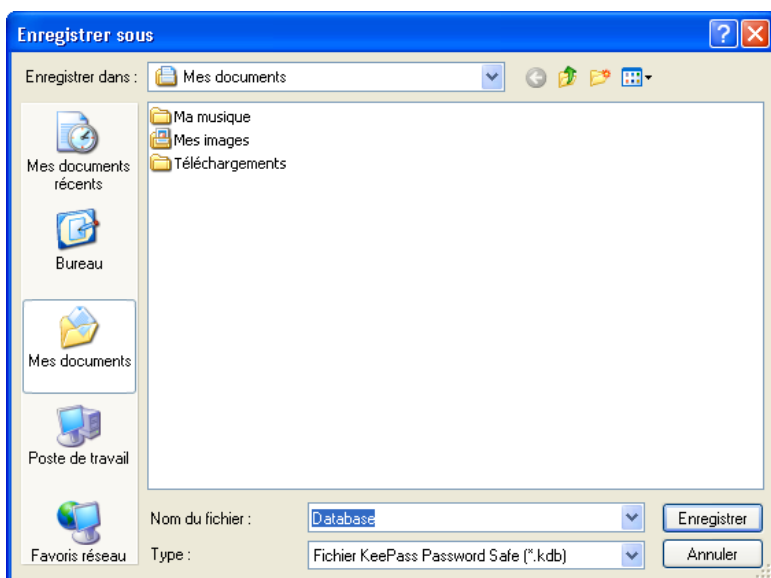


Figure 10: La fenêtre Enregistrer sous

**Deuxième étape. Saisissez** le nom désiré pour votre base de de mots de passe.

**Troisième étape. Cliquez** sur **Enregistrer** pour sauvegarder votre base de mots de passe.

**Astuce:** N'oubliez pas l'emplacement et le nom de fichier de votre base de mots de passe! Cela vous sera utile lorsque viendra le temps d'en faire une copie de sauvegarde.

Félicitations! Vous venez de créer et de sauvegarder votre base de mots de passe sécurisée. Vous pouvez désormais commencer à la remplir avec tous vos mots de passe actuels et futurs.

## 2.2. Comment ajouter une entrée

La fenêtre *Ajouter une entrée* vous permet d'ajouter les détails de vos comptes, vos mots de passe et d'autres renseignements importants à votre base de données. Dans l'exemple qui suit, vous ajouterez des entrées pour sauvegarder des mots de passe et des noms d'utilisateur associés à divers sites Internet et comptes de courriel.

**Première étape. Sélectionnez:** **Édition > Ajouter une entrée** à partir de la fenêtre *Password Safe* de **KeePass** pour activer la fenêtre *Ajouter une entrée*, comme suit:

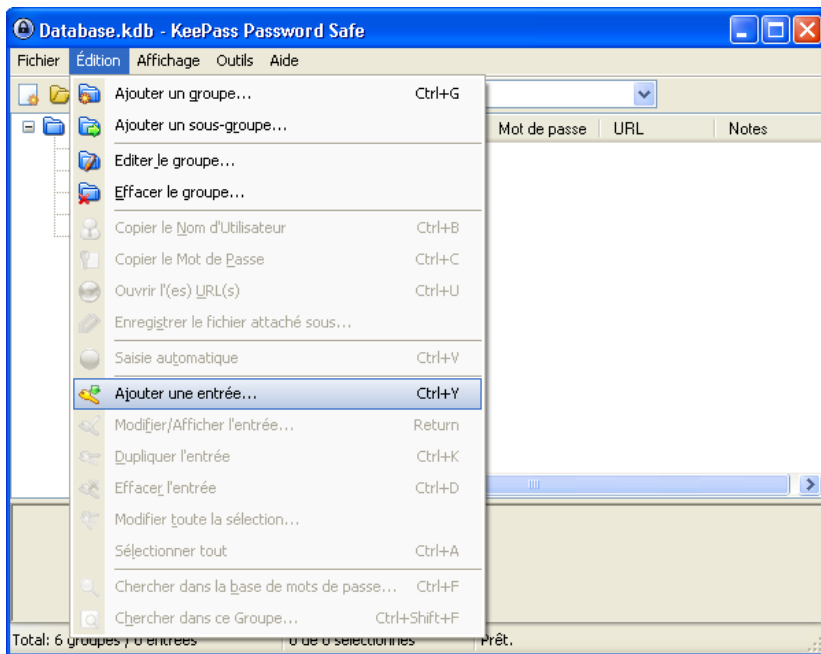


Figure 11: La fenêtre principale de KeePass, avec Édition > Ajouter une entrée sélectionné

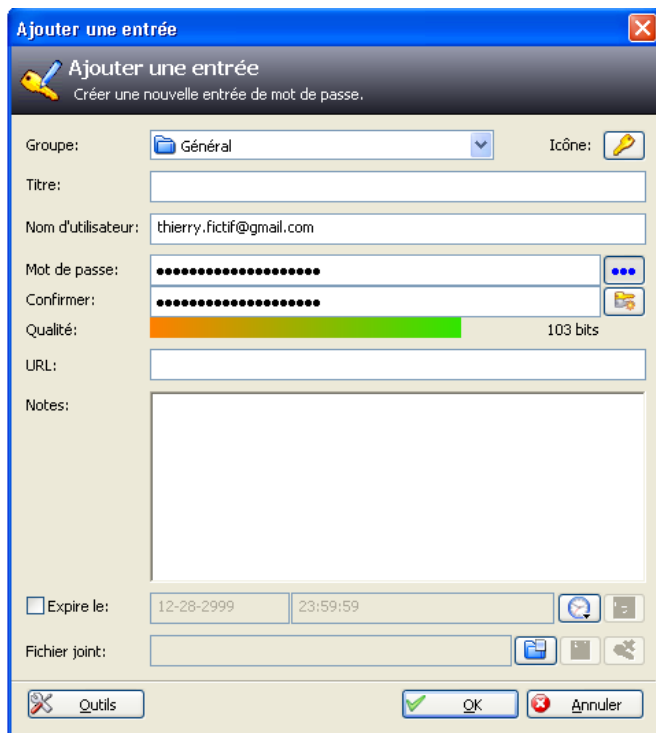


Figure 12: La fenêtre Ajouter une entrée

**Commentaire:** La fenêtre *Ajouter une entrée* vous présente plusieurs zones à remplir. Aucune de ces zones n'est obligatoire; les renseignements saisis ici servent principalement à faciliter l'utilisation. Ces renseignements pourraient s'avérer utiles dans des situations où vous seriez à la recherche d'une entrée en particulier.

Voici une courte explication pour chacune de ces zones de saisie:

- **Groupe:** KeePass vous permet de trier vos mots de passe dans des groupes prédéfinis. Par exemple, Internet est un bon emplacement pour stocker vos mots de passe associés à des comptes d'utilisateur sur des sites Internet. .
- **Titre:** Un titre pour décrire cette entrée de mot de passe. Par exemple: mot de passe Gmail.
- **Nom d'utilisateur:** Le nom d'utilisateur associé à cette entrée de mot de passe. Par exemple: securitybox@gmail.com
- **URL:** Le site Internet associé à cette entrée de mot de passe. Par exemple: https://mail.google.com
- **Mot de passe:** Cette fonctionnalité génère automatiquement un mot de passe aléatoire lorsque la fenêtre Ajouter une entrée est activée. Si vous enregistrez un nouveau compte de courriel, vous pouvez utiliser le mot de passe par défaut inscrit dans cette zone. Vous pouvez également utiliser cette fonction si vous désirez changer votre mot de passe existant pour un nouveau mot de passe généré par KeePass. Comme KeePass le conservera toujours pour vous, il n'est même pas nécessaire de voir ce mot de passe. Un mot de passe généré aléatoirement est considéré comme fort (c.-à-d. qu'un intrus aura de la difficulté à le deviner ou le déchiffrer).

La génération aléatoire sur demande d'un mot de passe sera expliquée à la prochaine section. Vous pouvez évidemment remplacer le mot de passe par défaut par un mot de passe de votre choix. Par exemple, si vous créez une entrée pour un compte qui existe déjà, il est souhaitable de saisir le mot de passe correspondant (existant) dans cette zone.

- **Confirmer:** La confirmation du mot de passe saisi.
- **Qualité:** Une barre de gradation qui mesure la force du mot de passe selon la longueur et le degré d'aléatoire. Plus la barre est verte, plus le mot de passe choisi est fort.
- **Notes:** C'est dans cette zone que vous saisissez des renseignements généraux concernant le compte ou le site pour lequel vous stockez de l'information. Par exemple : POP3 SSL, pop.gmail.com, Port 995; SMTP TLS, smtp.gmail.com, Port: 465\*

**Commentaire:** Le fait de créer ou modifier les entrées de mot de passe dans **KeePass** ne change pas réellement vos mots de passe! Considérez **KeePass** comme un livre d'adresses sécurisé où sont stockés vos mots de passe. Vous n'y trouvez que ce que vous y consignez, rien de plus.

Si vous sélectionnez *Internet* dans le menu défilant *Groupe*, votre entrée de mot de passe ressemblera peut-être à ceci :

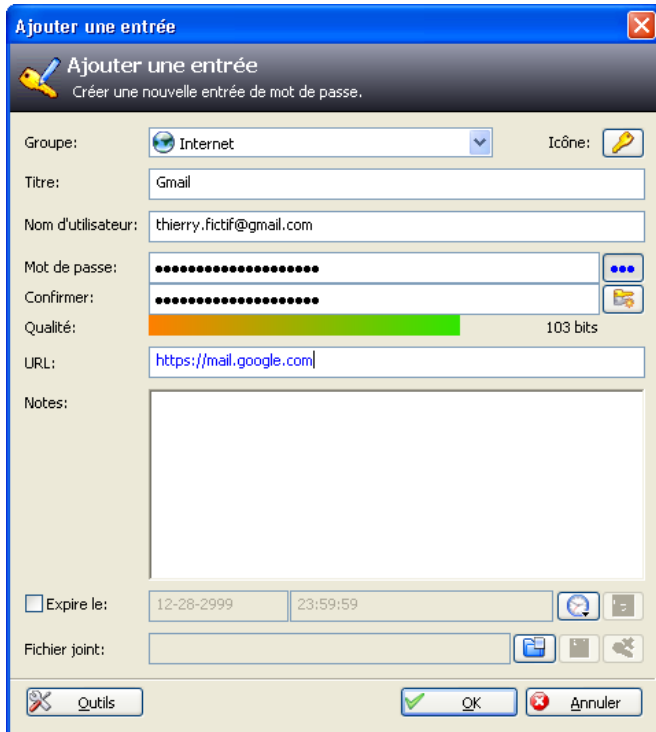


Figure 13: La fenêtre *Ajouter une entrée* remplie

**Deuxième étape.** Cliquez sur  pour sauvegarder cette entrée.

Votre mot de passe se trouve désormais dans le groupe **Internet**.

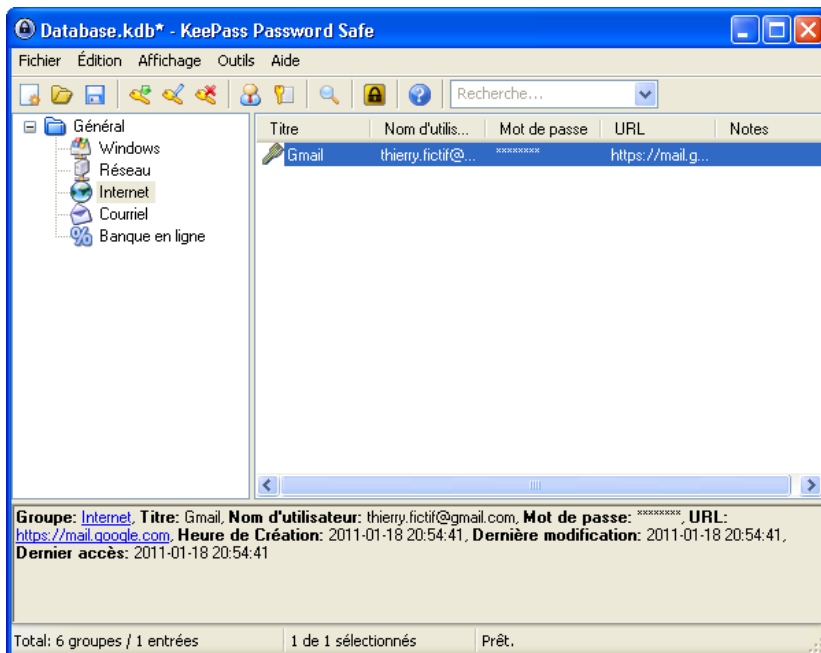


Figure 14: La fenêtre principale de *KeePass Password Safe*

**Commentaire:** Le panneau d'affichage au bas de cette fenêtre montre les renseignements inclus dans l'entrée sélectionnée. Cela comprend la création, l'édition et la date d'expiration, ainsi que les notes enregistrées dans cette entrée. Le mot de passe n'y est pas révélé.

- **Expire le:** Cochez cette option pour activer les zones de texte où vous pouvez spécifier une date limite de validité. Ce faisant, vous pouvez ajouter une note qui vous rappellera de changer votre mot de passe à date fixe (tous les

trois mois, par exemple). Lorsqu'un mot de passe aura dépassé sa date limite de validité, une petite croix rouge apparaîtra à côté de son nom, tel qu'illustré dans l'exemple ci-dessous:



Figure 15: Un exemple de clé expirée

## 2.3 Comment éditer une entrée

Il est possible d'éditer une entrée existante dans **KeePass**, et ce, en tout temps. Vous pouvez changer votre mot de passe (il est indiqué, pour des raisons de sécurité, de changer un mot de passe régulièrement tous les trois à six mois), ou modifier les autres détails inclus dans l'entrée du mot de passe.

Pour éditer une entrée, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez le bon *Groupe* dans la colonne de gauche pour activer les entrées qui y sont associées.

**Deuxième étape.** Sélectionnez l'entrée pertinente, puis **cliquez à droite** sur l'entrée sélectionnée pour activer la fenêtre ci-dessous :

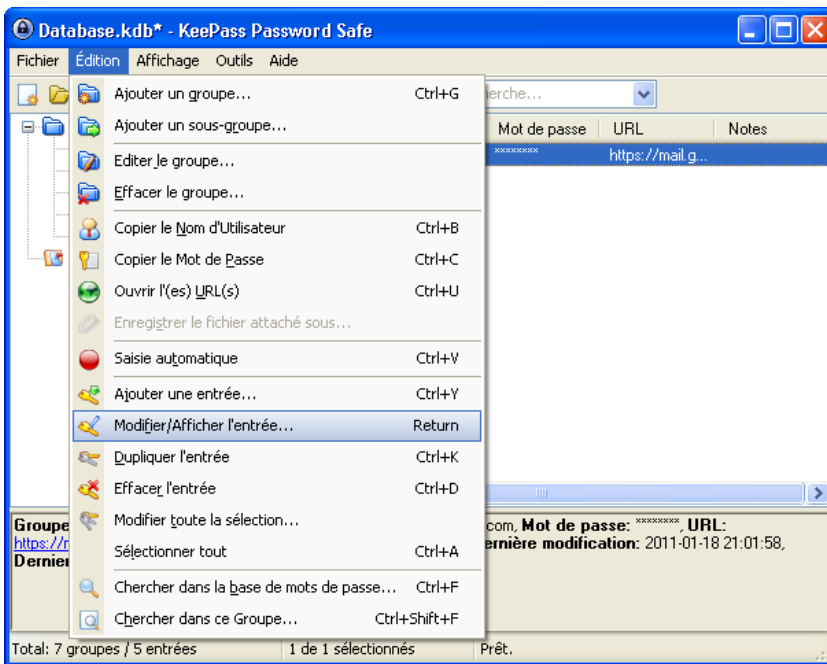


Figure 16: La fenêtre principale de KeePass Password Safe affichant le menu Édition


**Troisième.** Cliquez sur  pour sauvegarder tout changement, y compris le mot de passe.

Pour changer un mot de passe existant (que vous aviez préalablement créé vous-même) pour un nouveau mot de passe généré aléatoirement par KeePass, veuillez lire la section suivante.

## 2.4 Comment générer des mots de passe aléatoirement

De longs mots de passe aléatoires sont considérés comme forts dans le monde de la sécurité informatique. Leur nature aléatoire est fondée sur des principes mathématiques et il est pratiquement impossible pour un intrus de les deviner. **KeePass** fournit un *générateur de mot de passe* pour vous assister dans ce processus. Comme vous l'avez vu ci-dessus, un mot de passe aléatoire est automatiquement généré lorsque vous créez une nouvelle entrée. Cette section vous montrera comment en générer un par vous-même.

**Commentaire:** Le *générateur de mot de passe* peut être activé depuis les fenêtres *Ajouter une entrée* et *Modifier/Afficher l'entrée*. Sinon, sélectionnez: **Outils > Générateur de mots de passe**.

**Première étape.** Cliquez sur  depuis la fenêtre *Ajouter une entrée* ou la fenêtre *Modifier/Afficher l'entrée*, pour afficher

la fenêtre *Générateur de mots de passe* illustrée ci-dessous :

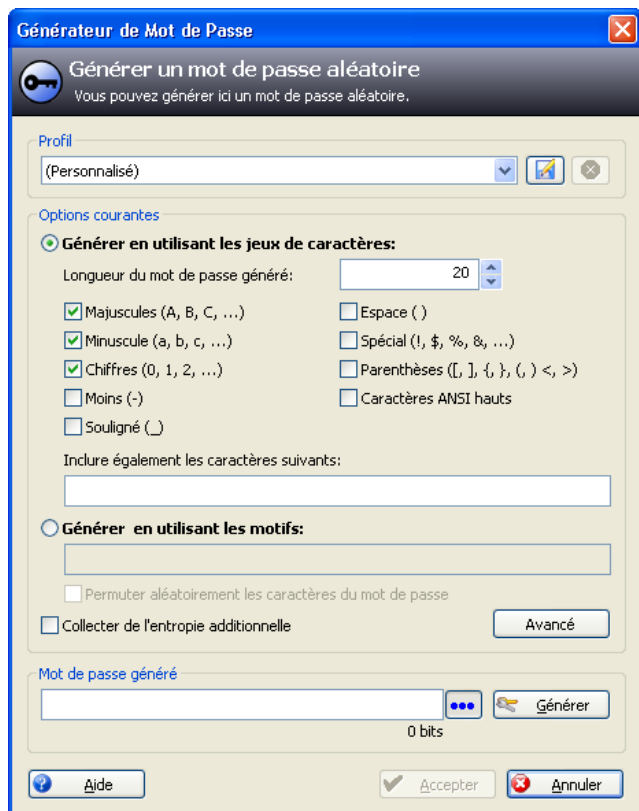



Figure 17: La fenêtre *Générateur de mots de passe*

La fenêtre *Générateur de mots de passe* présente plusieurs options pour générer un mot de passe. Vous pouvez préciser la longueur du mot de passe souhaité, les jeux de caractères utilisés pour le créer, et bien plus. Pour les fins de cet exemple, conservons les paramètres par défaut qui nous sont présentés. Cela signifie que le mot de passe généré comportera 20 caractères et sera composé de lettres majuscules et minuscules, ainsi que de chiffres.

**Deuxième étape.** Cliquez sur  pour entamer le processus. Lorsque celui-ci sera terminé, **KeePass** vous présentera le mot de passe généré.

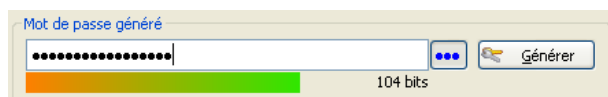

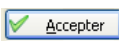


Figure 18: La rubrique *Mot de passe généré* de KeePass

**Commentaire:** Vous pouvez visionner le mot de passe généré en **cliquant** . Cependant, cela comporte un risque de sécurité, comme nous l'avons déjà mentionné. Au fond, vous n'aurez jamais vraiment besoin de voir le mot de passe généré. Nous y reviendrons à la section **3.0 Comment utiliser les mots de passe** <sup>[60]</sup>.

**Troisième étape.** Cliquez sur  pour accepter le mot de passe et retourner à la fenêtre *Ajouter une entrée* illustrée ci-dessous:

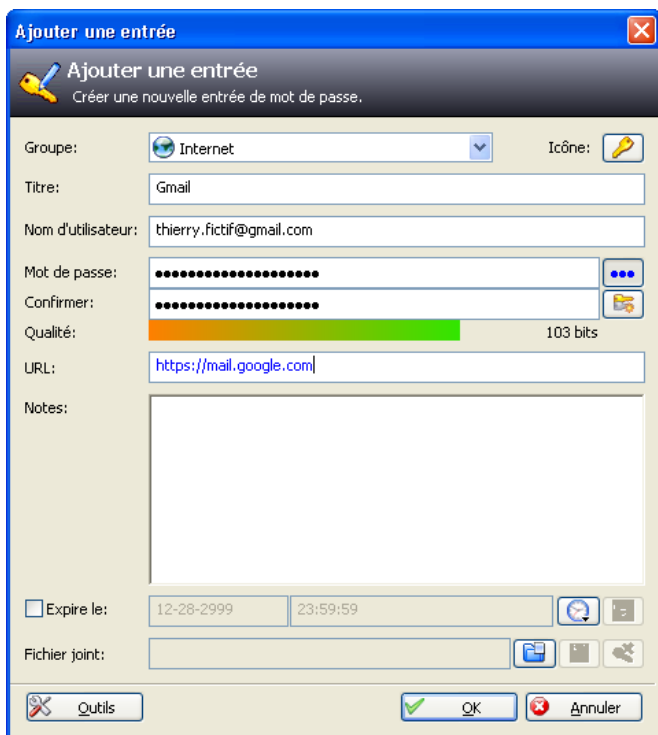
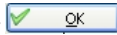



Figure 19: La fenêtre Ajouter une entrée

**Quatrième étape.** Cliquez sur  pour sauvegarder cette entrée.

**Cinquième étape.** Sélectionnez: **Fichier > Enregistrer** pour sauvegarder la base de données ainsi mise à jour.

## 2.5 Comment fermer, réduire ou restaurer KeePass

Vous pouvez réduire ou fermer le logiciel **KeePass** en tout temps. Lorsque vous souhaitez rouvrir ou restaurer le programme, une invite vous demandera de saisir de nouveau votre mot de *passse principale*.

**KeePass** se réduit automatiquement et cet icône  s'affiche dans votre barre de tâches système (dans le coin inférieur droit de votre écran).

**KeePass** vous permet également de verrouiller le programme en suivant les étapes décrites ci-dessous:

**Première étape.** Sélectionnez: **Fichier > Verrouiller l'espace de travail** pour afficher la fenêtre suivante:

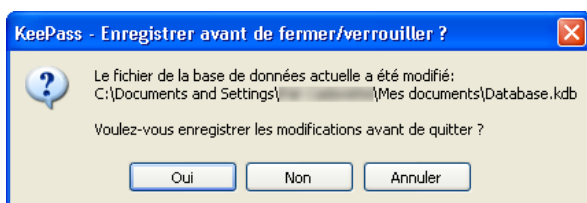



Figure 20: La fenêtre Enregistrer avant de fermer/verrouiller de KeePass

**Deuxième étape.** Cliquez sur  pour sauvegarder l'information et désactiver la console **KeePass**, qui devrait maintenant ressembler à la *figure 2*. Cet icone apparaît désormais dans votre *barre de tâches système*:



**Première étape.** **Double-cliquer** sur cet icone pour restaurer **KeePass** à la grandeur normale et afficher la fenêtre suivante:





Figure 21: La fenêtre Ouvrir base de données Database.kdb

**Troisième étape.** Saisissez votre *Mot de passe principal* pour ouvrir KeePass.

Pour fermer KeePass:

**Première étape.** Sélectionnez: **Fichier > Quitter** pour fermer complètement le programme KeePass.

Si des changements ont été apportés à la banque de mots de passe mais n'ont pas été sauvegardés, KeePass vous invitera à enregistrer la sauvegarde.

## 2.6 Comment créer une copie de sauvegarde de la base de mots de passe

Le fichier de la base de mots de passe KeePass qui se trouve sur votre ordinateur est désigné par l'extension de fichier .kdb. Vous pouvez copier ce fichier sur une clé USB. Personne d'autre que vous ne sera en mesure d'ouvrir la base de donnée, à moins de connaître le mot de passe principal.

**Première étape.** Sélectionnez: **Fichier > Enregistrez sous** depuis la fenêtre principale, puis sauvegardez une copie de la base de données à un autre emplacement.

Il est possible d'exécuter le programme KeePass depuis une clé USB. Veuillez consulter le guide pratique [KeePass Portable](#) [61].

## 2.7 Comment réinitialiser votre mot de passe principal

Vous pouvez changer votre *mot de passe principal* en tout temps. Pour ce faire, il faut d'abord ouvrir la banque de mots de passe.

**Première étape.** Sélectionnez: **Fichier > Modifier la clé maître**

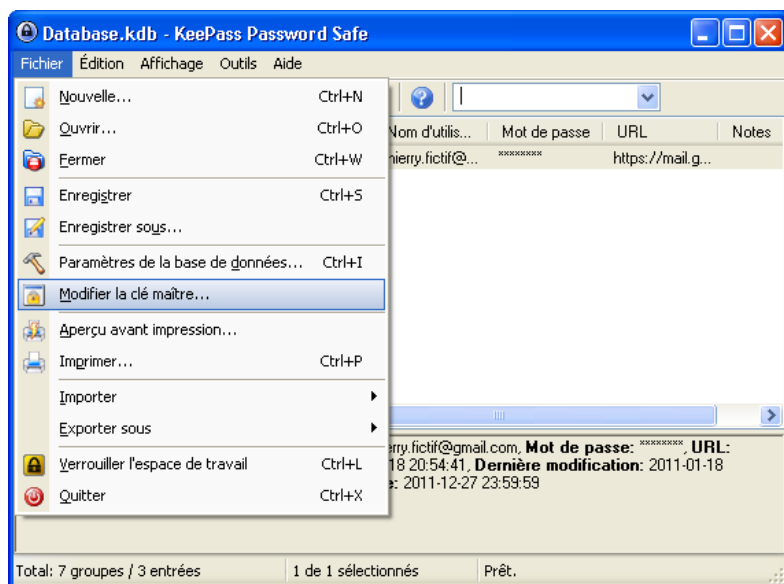


Figure 22: Le menu fichier avec l'option Modifier la clé maître sélectionnée

**Deuxième étape.** Saisissez deux fois votre nouveau *Mot de passe principal*.

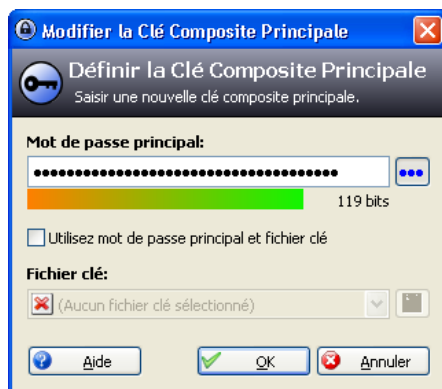


Figure 23: La fenêtre Modifier la clé composite principale

## Comment utiliser les mots de passe

### 3.0 Comment utiliser les mots de passe

Puisqu'un mot de passe sécurisé est difficile à mémoriser, KeePass vous permet de le copier depuis la base de données

et le coller directement dans le compte ou le site Internet qui le requiert. Pour plus de sécurité, un mot de passe copié ne restera pas plus de 10 secondes dans le presse-papiers, alors il est conseillé d'avoir déjà ouvert le compte ou le site Internet pour que vous puissiez y copier rapidement votre mot de passe.

**Première étape.** Cliquez à droite sur l'entrée de mot de passe appropriée pour activer le menu contextuel.

**Deuxième étape.** Sélectionnez : Copier le Mot de passe dans le Presse-Papiers comme suit:

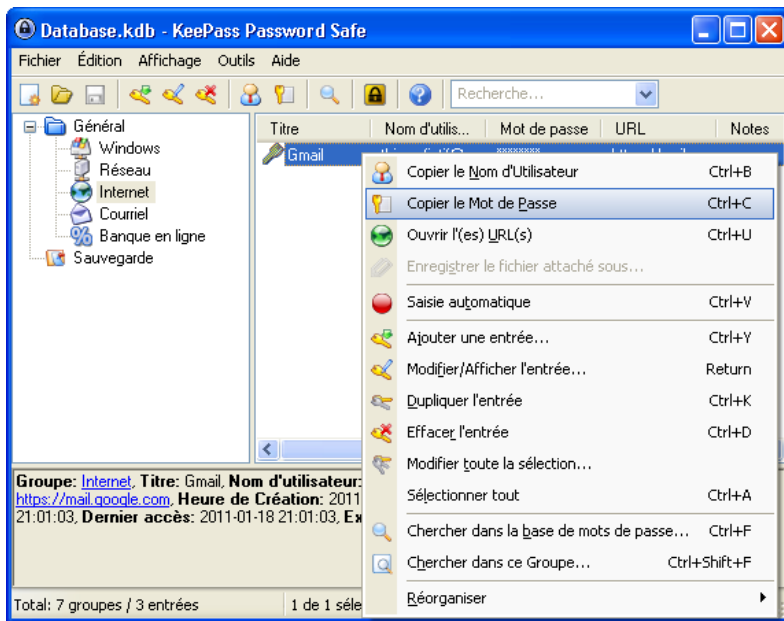


Figure 1: La fenêtre de KeePass Password Safe

**Troisième étape.** Rendez-vous dans le compte ou sur le site pertinent et collez le mot de passe dans la zone appropriée :

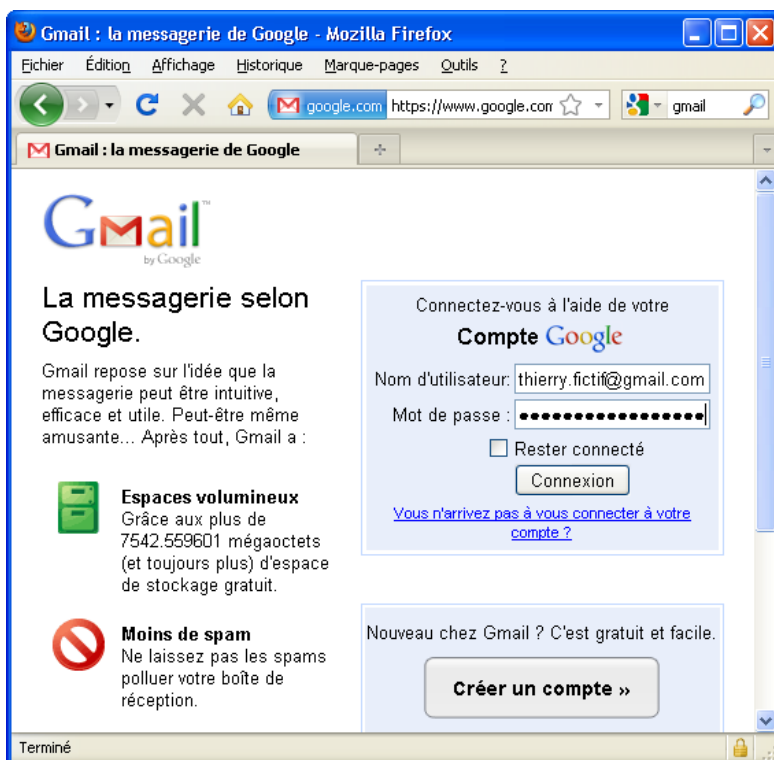


Figure 2: Un compte de courriel Gmail affichant un mot de passe copié-collé

**Astuce:** Pour copier, coller et changer de fenêtre efficacement, utilisez les raccourcis de clavier. **Pressez et maintenez enfoncée** la touche **Ctrl**, puis appuyez sur la touche **C** pour copier un mot de passe. **Pressez et maintenez enfoncée** la touche **Ctrl**, puis appuyez sur la touche **V** pour coller ce mot de passe. **Pressez et maintenez enfoncée** la touche **Alt**, puis appuyez sur la touche **Tab** pour naviguer entre les programmes et les fenêtres ouvertes.

**Commentaire:** En utilisant constamment **KeePass**, vous n'avez pas besoin de voir votre mot de passe, ni même de le connaître. La fonction copier/coller suffit à transférer le mot de passe de la base de données à la fenêtre appropriée. Si vous utilisez la fonction *Générateur de mot de passe* et transférez ensuite ce mot de passe dans un nouveau compte de courriel, vous utiliserez un mot de passe que vous n'aurez en fait jamais vu. Et ça fonctionne!

## Faq et questions récapitulatives

## 4.0 Faq et questions récapitulatives

**KeePass** KeePass semble être un programme facile à utiliser pour Nikolai et Elena. Le seul aspect qui leur paraît plus difficile est de prendre l'habitude de créer de nouveaux mots de passe avec **KeePass**. Elena a du mal à se faire à l'idée qu'elle ne verra jamais plus de mots de passe, mais c'est définitivement plus facile que de devoir s'en rappeler!

**Q:** Nikolai, j'ai été surprise de constater à quel point il est facile de se servir de **KeePass**. Par contre, si jamais par malheur j'oubliais mon mot de passe principal, y aurait-il une façon d'accéder à **KeePass** pour récupérer ma banque de mots de passe?

**A:** Elle est facile celle-là, Elena! Non. Désolé, il n'y a rien à faire dans cette situation. Mais pour prendre les choses du bon côté, au moins, personne d'autre ne sera en mesure d'accéder à ta banque de mots de passe! Pour empêcher que cela ne se produise, tu peux toujours employer l'une ou l'autre des méthodes pour se souvenir d'un mot de passe qui sont suggérées au chapitre **3. Créer et sauvegarder des mots de passe sûrs** <sup>[54]</sup> du livret pratique

**Q:** Et si je désinstalle **KeePass**, qu'advient-il de mes mots de passe?

**A:** Le programme sera supprimé de ton ordinateur, mais ta base de données (stockée dans le fichier `.kdb`) s'y trouvera toujours. Tu pourras ouvrir ce fichier en tout temps si tu réinstalles **KeePass** plus tard.

**Q:** Je crois que j'ai supprimé le fichier de la base de données par erreur!

**A:** J'espère que tu avais fait une copie de sauvegarde! Aussi, assure-toi que tu n'as pas simplement oublié l'emplacement de ton fichier. Exécute une recherche sur ton ordinateur pour trouver un fichier comprenant l'extension `.kdb`. Si tu l'as effectivement supprimé, jette un coup d'œil au Guide pratique **Recuva** <sup>[62]</sup>. Cela pourrait t'aider à retrouver ton fichier.

## 4.1 Questions récapitulatives

- Qu'est-ce qui constitue un mot de passe fort?
- Comment puis-je modifier une entrée de mot de passe existante dans **KeePass**?
- Comment puis-je générer un mot de passe de 30 caractères dans **KeePass**?

## TrueCrypt - stockage de fichiers sécurisé

### Short Description:

**TrueCrypt** protège vos données en empêchant quiconque ne dispose pas du bon mot de passe d'y accéder. C'est en quelque sorte un «coffre-fort» électronique où vous rangez vos fichiers en sûreté.

### Online Installation Instructions:

#### Pour télécharger TrueCrypt

- Lisez la courte introduction aux **Guides pratiques** <sup>[1]</sup>
- Cliquez sur l'icône **TrueCrypt** ci-dessous pour ouvrir la page de téléchargement [www.truecrypt.org/downloads](http://www.truecrypt.org/downloads)
- Sous la section **Latest Stable Version - Windows**, cliquez sur le bouton **Download**
- Sauvegardez le fichier d'installation sur votre ordinateur à un emplacement de votre choix, puis cliquez dessus pour lancer l'installation.
- Lisez attentivement les consignes d'installation avant de continuer
- Vous pouvez supprimer l'exécutable après l'installation.

#### TrueCrypt:



<sup>[63]</sup>

#### Pour utiliser TrueCrypt en français

- Installez KeePass en suivant les consignes indiquées à la section **2.0 Comment installer TrueCrypt** <sup>[64]</sup>
- Rendez-vous à la **page web des traductions de TrueCrypt** <sup>[65]</sup>
- Localisez le fichier `.zip` de traduction française **langpack-fr-0.1.0-for-truecrypt-7.0a** et sauvegardez-le à un emplacement de votre choix.
- Décompactez le fichier `.zip`, et copiez le fichier `Language.fr.xml` dans le répertoire où **TrueCrypt** est installé (habituellement `C:/Program Files/TrueCrypt`).
- Démarrez **TrueCrypt**. Le logiciel devrait s'ouvrir en français. Sinon, allez au menu `Settings > Language` et sélectionnez **Français**.

#### Site Internet

[www.truecrypt.org](http://www.truecrypt.org) <sup>[66]</sup>

#### Configuration requise

- Windows 2000/XP/2003/Vista/7
- Les droits d'administration sont nécessaires pour installer le logiciel et créer des volumes chiffrés, mais pas pour accéder aux volumes existants.

#### Version utilisée pour rédiger ce guide

- 7.0a

#### Licence

- FLOSS (Free/Libre & Open Source Software)

## Lecture préalable

- Livret pratique Security in-a-box, chapitre **4. Protéger les données sensibles stockées sur votre ordinateur** <sup>[67]</sup>

## Niveau

- (Volumes Standards): 1 : Débutant, 2 : Moyen, **3 : Intermédiaire**, 4 : Expérimenté, 5 : Avancé
- (Volumes cachés): 1 : Débutant, 2 : Moyen, 3 : Intermédiaire, **4 : Expérimenté**, 5 : Avancé

## Temps d'apprentissage:

- (Volumes Standards): 30 minutes
- (Volumes cachés): 30 minutes

\*\*Ce que vous apportera l'utilisation de cet outil \*\*:

- La capacité de protéger efficacement vos fichiers de toute intrusion et de tout accès non autorisé.
- La capacité de stocker facilement des copies de sauvegarde de vos fichiers importants, et ce, de façon sécurisée.

## Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

**Commentaire:** Nous recommandons fortement **TrueCrypt** pour **GNU Linux** et **Mac OS**.

Plusieurs distributions de **GNU Linux**, par exemple **Ubuntu** <sup>[68]</sup>, supportent le chiffrement/déchiffrement à la volée du disque au complet. Vous pouvez choisir d'utiliser cette fonction standard à l'installation du système. Vous pouvez également ajouter la fonction de chiffrement à votre système **Linux** en utilisant l'intégration de **dm-crypt** <sup>[69]</sup> et **cryptsetup et LUKS** <sup>[70]</sup>. Une autre approche consiste à utiliser **ScramDisk pour Linux SD4L** <sup>[71]</sup>, un programme gratuit et de source libre de chiffrement/déchiffrement à la volée.

Pour **Mac OS**, vous pouvez utiliser **FileVault**, qui est intégré au système d'exploitation, pour chiffrer et déchiffrer à la volée le contenu de votre répertoire *Home* et tous ses dossiers. On trouve également un programme gratuit et de source libre **Encrypt This** <sup>[72]</sup>. Ce programme permet de chiffrer des fichiers choisis dans une image de disque .DMG.

Il existe plusieurs programmes de chiffrement pour **Microsoft Windows**. Nous recommandons ceux-ci:

- **FREE CompuSec** <sup>[73]</sup> est un programme gratuit, propriétaire, de chiffrement/déchiffrement à la volée. Il peut, chiffrer un disque dur, une clé USB ou un CD en partie ou au complet. Le module **DataCrypt** de **CompuSec** peut être utilisé pour chiffrer des fichiers individuels.
- **CryptoExpert 2009 Lite** <sup>[74]</sup> est un programme gratuit, propriétaire, de chiffrement/déchiffrement à la volée qui crée des volumes chiffrés, à la manière de **TrueCrypt**.
- **AxCrypt** <sup>[75]</sup> est un programme gratuit et de source libre qui permet de chiffrer des fichiers individuels.
- **Steganos LockNote** <sup>[76]</sup> est un programme gratuit et de source libre. Il peut être utilisé pour chiffrer et déchiffrer n'importe quel texte. Le texte sera stocké dans l'application **LockNote**: Le mécanisme qui permet de chiffrer ou de déchiffrer une note est incorporé au fichier. **LockNote** est portable et aucune installation n'est requise.

## 1.1 À propos de cet outil

**TrueCrypt** protégera vos données en les verrouillant derrière un mot de passe que vous créerez vous-même. Attention : Si vous oubliez le mot de passe, vous perdrez l'accès à vos données! **TrueCrypt** utilise un processus de chiffrement pour protéger vos fichiers (veuillez vous assurer que le chiffrement est légal dans votre pays!). Au lieu de chiffrer les fichiers existants, **TrueCrypt** crée une section protégée sur votre ordinateur, un *volume* chiffré, où vous pouvez ensuite stocker des fichiers de façon sécurisée.

**TrueCrypt** offre la possibilité de créer un volume standard ou un volume caché. D'une manière ou d'une autre, vos fichiers resteront confidentiels, mais un volume caché vous permet de dissimuler vos données les plus importantes derrière des données moins délicates, ce qui les protège même lorsque vous êtes forcé à ouvrir votre volume **TrueCrypt** standard. Le présent guide explique comment fonctionnent les deux types de volume.

### Offline Installation Instructions :

#### Pour installer TrueCrypt

- \*Lisez la courte **Introduction** aux **Guides pratiques** <sup>[1]\*\*</sup>
- **Cliquez sur l'icône TrueCrypt ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.

TrueCrypt:



<sup>[77]</sup> [ER](#) <sup>[78]</sup>

# Comment installer TrueCrypt et créer des volumes standards

Sommaire des sections de cette page:

- **[2.0 Comment installer TrueCrypt](#)**
- **[2.1 À propos de TrueCrypt](#)**
- **[2.2 Comment créer un volume standard](#)**
- **[2.3 Comment créer un volume standard sur une clé USB](#)**

- 2.4 Comment créer un volume standard (suite)

## 2.0 Comment installer TrueCrypt

**Première étape.** Double-cliquez sur TrueCrypt Setup 7.0a ; si la boîte de dialogue *Fichier ouvert - Avertissement de sécurité* s'affiche, cliquez sur  pour afficher la fenêtre **TrueCrypt License**.

**Deuxième étape.** Cochez l'option *I accept and agree to be bound by the license terms* pour activer le bouton *Accept*; cliquez sur  pour afficher la fenêtre suivante:

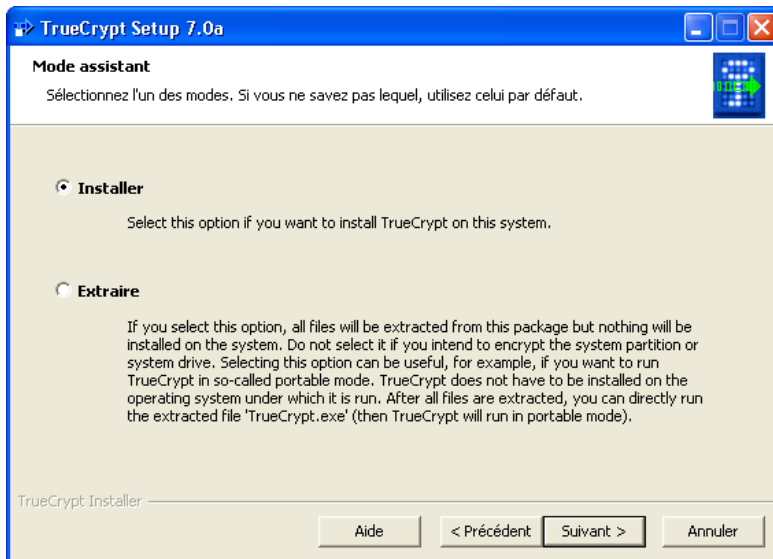


Figure 1: Le Mode assistant en mode d'installation par défaut

- Le mode *Installer*: Cette option est pour les utilisateurs qui ne souhaitent pas cacher le fait qu'ils utilisent **TrueCrypt** sur leur ordinateur.
- Le mode *Extraire*: Cette option est pour les utilisateurs qui souhaitent transporter une version portable de **TrueCrypt** sur une clé USB et qui ne souhaitent pas installer **TrueCrypt** sur leur ordinateur.

**Commentaire:** Certaines options (par exemple, le chiffrement de partitions entières et de disques entiers) ne fonctionneront pas si **TrueCrypt** est extrait mais non installé.

**Commentaire:** Même si le mode *Installer* par défaut est recommandé ici, vous voudrez peut-être utiliser la version portable de **TrueCrypt** ultérieurement. Pour en savoir plus sur le mode **TrueCrypt Traveller**, veuillez consulter le chapitre [TrueCrypt mode Traveler](#) [79].

**Troisième étape.** Cliquez sur  pour afficher la fenêtre suivante:

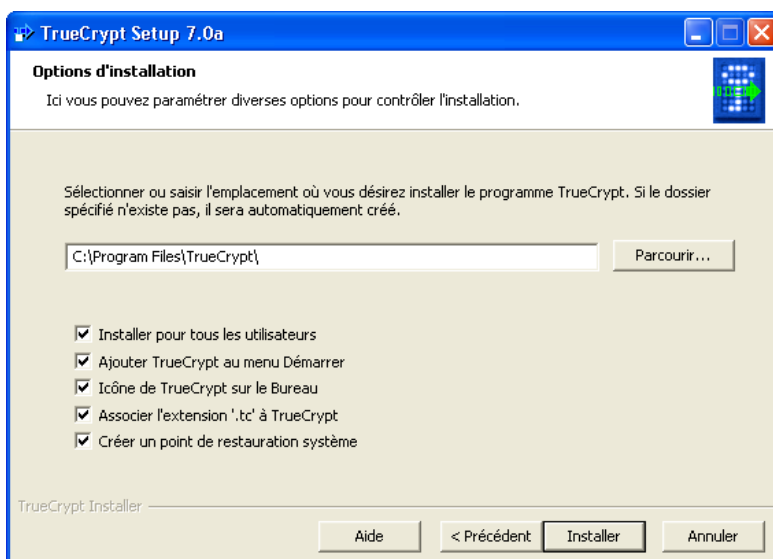


Figure 2: La fenêtre Options d'installation

**Quatrième étape.** Cliquez sur  pour afficher la fenêtre *Installation en cours* et lancer l'installation de **TrueCrypt** sur votre système.

**Cinquième étape.** Cliquez sur  pour afficher la fenêtre suivante:

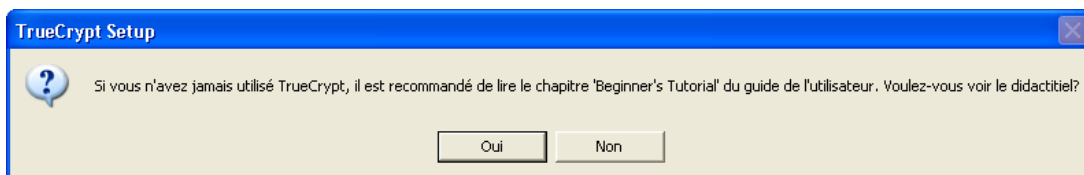




Figure 3: La boîte de dialogue de confirmation de l'installation de TrueCrypt

**Sixième étape.** Cliquez sur  pour ouvrir le site Internet de **TrueCrypt** et finaliser l'installation de \*TrueCrypt\*\*, puis cliquez sur .

**Commentaire:** Il est recommandé à tous les utilisateurs de consulter la documentation d'aide fournie par **TrueCrypt**.

## 2.1 À propos de TrueCrypt

**TrueCrypt** est conçu pour sécuriser vos fichiers en bloquant l'accès à quiconque ne dispose pas du mot de passe nécessaire. Le logiciel fonctionne un peu comme un "coffre-fort" électronique en vous permettant de verrouiller vos fichiers de telle sorte que seule une personne disposant du bon mot de passe puisse y accéder. **TrueCrypt** vous permet de créer des *volumes*, ou des sections de votre ordinateur où vous pouvez stocker des fichiers de façon sécurisée. Lorsque vous créez des données dans ces volumes, ou lorsque vous y transférez des données, TrueCrypt chiffre automatiquement cette information. Lorsque vous ouvrez ou déplacez ces fichiers, le programme les déchiffre automatiquement. Ce processus s'appelle chiffrement/déchiffrement à la volée.

## 2.2 Comment créer un volume standard

**TrueCrypt** vous donne le choix de créer deux types de volumes: *caché* et *standard*. Dans cette section section, nous verrons comment créer un *volume standard* pour y stocker vos fichiers.

Pour commencer à utiliser **TrueCrypt** en créant un *volume standard*, suivez les étapes énumérées ci-dessous:

**Première étape.** Double-cliquez  ou Sélectionnez Démarrer > Programmes > TrueCrypt > TrueCrypt pour ouvrir TrueCrypt.

**Deuxième étape.** Sélectionnez un lecteur dans la liste du panneau principal TrueCrypt illustré ci-dessous:

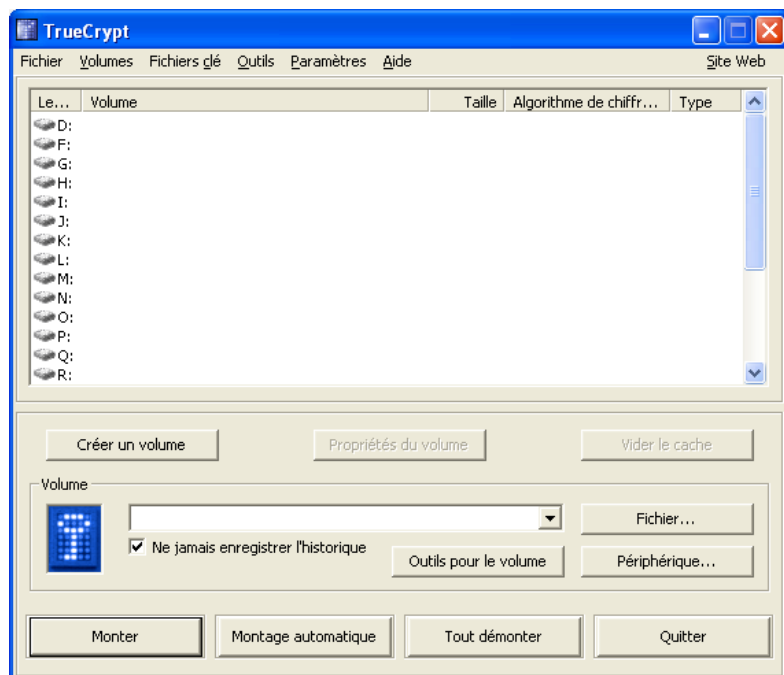


Figure 4: La console TrueCrypt


**Troisième étape.** Cliquez sur  pour activer l'Assistant de création de volume TrueCrypt, illustré ci-dessous:



Figure 5: L'Assistant de création de volume TrueCrypt

La figure 5 vous présente trois options pour créer un *volume standard*. Dans ce chapitre, nous aborderons la *Création d'un conteneur chiffré (Create an encrypted file container)*. Veuillez consulter la documentation de [TrueCrypt](#) [80] pour obtenir les descriptions des deux autres options.

**Quatrième étape.** Cliquez sur  pour afficher la fenêtre suivante:



Figure 6: La fenêtre Type de volume

La fenêtre *Assistant de création de volume TrueCrypt - Type de volume* offre le choix entre un *volume standard* et un *volume caché*.

**Important:** Voir la section [Volumes cachés](#) [81] du présent guide pour plus d'information sur la création d'un *volume caché*.

**Cinquième étape.** Cochez l'option *Volume TrueCrypt Standard*.

**Sixième étape.** Cliquez sur  pour afficher la fenêtre suivante:



Figure 7: L'Assistant de création de volume TrueCrypt affichant le panneau Emplacement du volume

Vous pouvez déterminer où vous aimeriez stocker votre *volume standard* dans la fenêtre de l'Assistant de création de volume - *Emplacement du volume*. Ce fichier peut être stocké comme n'importe quel autre type de fichier

**Septième étape.** Saisissez le nom du fichier dans la zone de texte ou cliquez sur  pour afficher la fenêtre suivante:

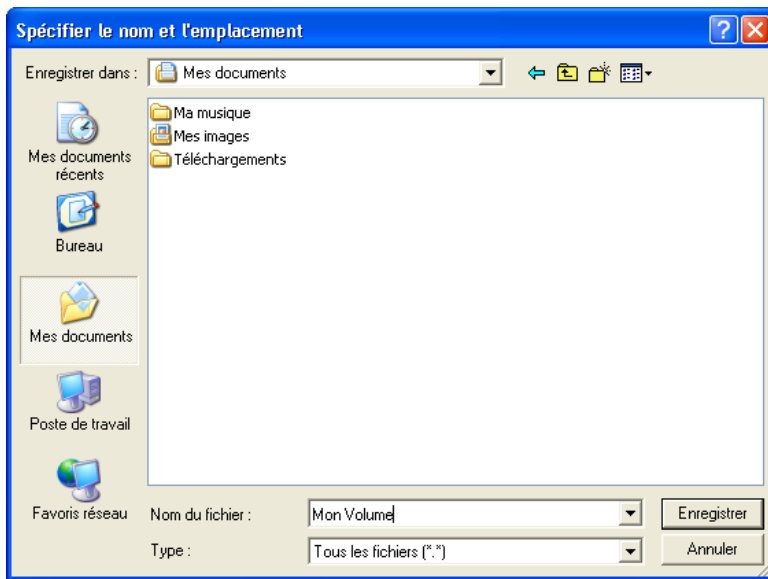


Figure 8: La fenêtre Spécifier le nom et l'emplacement

**Commentaire:** Un volume **TrueCrypt** est contenu à l'intérieur d'un fichier normal. Cela signifie qu'il peut être déplacé, copié et même supprimé! Il est donc très important de se rappeler le nom et l'emplacement du fichier. Cependant, vous devez choisir un nouveau nom de fichier pour le volume que vous créez (veuillez également consulter la section [2.3 Comment créer un volume standard sur une clé USB](#)). Pour les fins de cet exercice, nous créerons notre *volume standard* dans le répertoire *Mes documents*, et nous nommerons le fichier *Mon volume* (voir Figure 8, ci-dessus).

**Astuce:** Vous pouvez utiliser n'importe quel nom de fichier et type d'extension. Par exemple, vous pouvez nommer votre volume standard *recettes.doc* pour lui donner l'apparence d'un document *Word*, ou *vacances.mpeg* pour lui donner l'apparence d'un d'un fichier vidéo. C'est un moyen par lequel vous pouvez dissimuler l'existence d'un volume standard.

**Huitième étape.** Cliquez sur  pour fermer la fenêtre *Spécifier le nom et l'emplacement* et revenir à l'Assistant de création de volume:

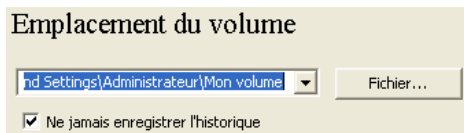


Figure 9: L'Assistant de création de volume de TrueCrypt affichant le panneau Emplacement du volume

**Neuvième étape.** Cliquez sur  pour afficher la figure 10.

## 2.3 Comment créer un volume standard sur une clé USB

Pour créer un volume **TrueCrypt** standard sur une clé USB, suivez les étapes 1 à 3 décrites à la section [2.2 Comment créer un volume standard](#) afin d'activer la fenêtre *Type de volume*. Au lieu de choisir *Mes documents* comme emplacement, **naviguez** jusqu'à votre clé USB. **Nommez** ensuite votre fichier et **créez** votre *volume standard* à cet emplacement.

## 2.4 Comment créer un volume standard (suite)

À ce point, il faut déterminer une méthode de chiffrement spécifique (ou *algorithme* selon le vocabulaire du logiciel) pour encoder les données qui seront stockées dans le *volume standard*.





Figure 10: Le panneau Options de chiffrement

**Commentaire:** Vous pouvez laisser les options par défaut telles quelles. Tous les algorithmes présentés dans les deux options sont considérés sûrs.

**Dixième étape.** Cliquez sur  pour afficher la fenêtre *Taille du volume* de l'Assistant de création de volume TrueCrypt.

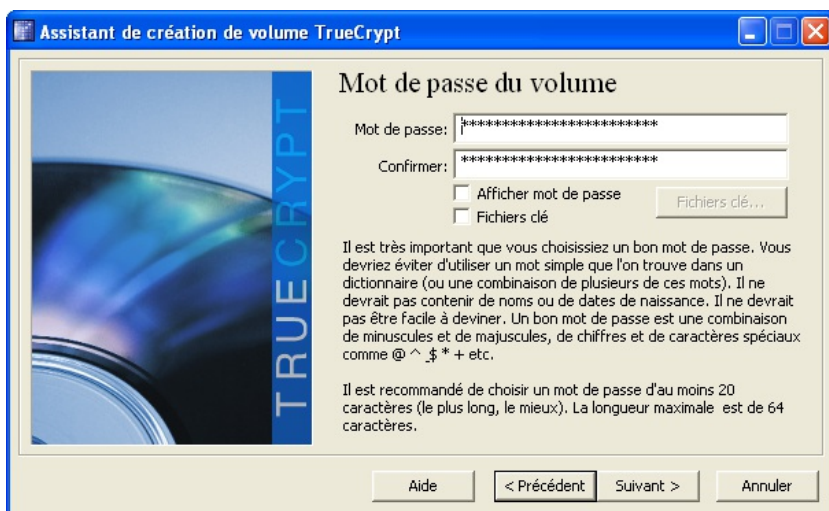


Figure 11: La fenêtre Taille du volume

La fenêtre *Taille du volume* vous permet de préciser la taille du *volume standard*. Dans cet exemple, le volume est réglé à 10 Mo. Vous pouvez toutefois déterminer la taille qui vous convient. Prenez en considération les documents et les types de fichiers que vous voudrez stocker, ainsi que leur poids, et déterminez ensuite une taille de volume appropriée.

**Astuce:** Si vous avez l'intention de créer une copie de sauvegarde de votre *volume standard* sur un CD, vous devriez régler votre volume à 700 Mo.

**Onzième étape.** Saisissez la taille de volume souhaitée dans la zone de texte, puis cliquez sur  pour afficher la fenêtre suivante:



\*Figure 12: La fenêtre Mot de passe du volume \*

**Important:** Le choix d'un mot de passe fort et sécuritaire est l'une des tâches les plus importantes à accomplir lors du processus de création d'un *volume standard*. Un bon mot de passe protégera efficacement un volume chiffré: plus votre mot de passe est fort, mieux votre volume sera protégé. Vous n'êtes pas obligé de créer vos propres mots de passe, ou même de vous en rappeler, si vous utilisez un programme de génération automatique de mots de passe comme **KeepPass**. Veuillez consulter le Guide pratique **KeepPass** [82] pour obtenir des renseignements sur la création et le stockage de mots de passe.

**Douzième étape.** Saisissez votre mot de passe, puis **saisissez-le** à nouveau dans les zones de texte *Mot de passe* et *Confirmer*.

**Important:** Le bouton *Suivant* demeurera désactivé tant et aussi longtemps que les mots de passe saisis dans les deux zones de texte ne correspondront pas. Si le mot de passe que vous avez choisi n'est pas particulièrement sûr, un message d'avertissement apparaîtra. Il est conseillé, dans ce cas, de changer de mot de passe! Cela dit, **TrueCrypt** fonctionnera tout de même avec le mot de passe que vous avez choisi, même si vos données ne seront pas particulièrement bien sécurisées.

**Treizième étape.** Cliquez sur  pour afficher la fenêtre suivante:

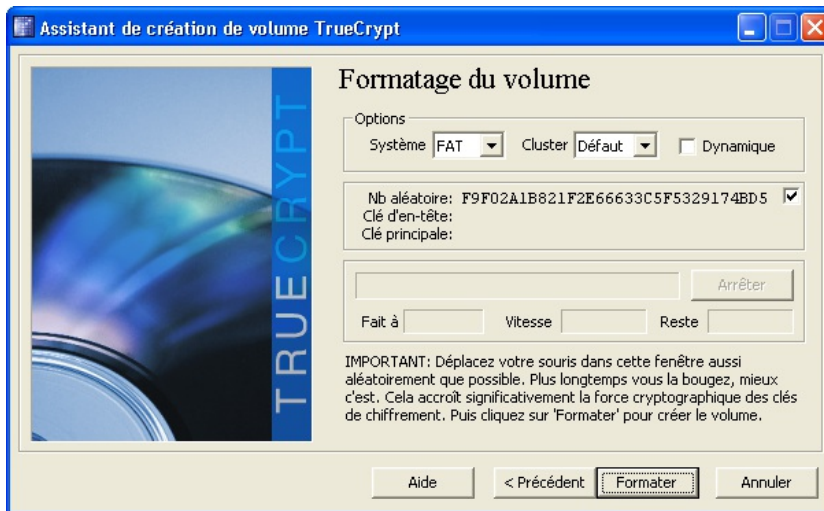



Figure 13: La fenêtre *Formatage du volume*

**TrueCrypt** est maintenant prêt à créer un volume standard. Bougez votre souris aléatoirement au dessus de la fenêtre de l'*Assistant de création de volume TrueCrypt* pendant au moins 30 secondes. Plus vous bougez votre souris longtemps, meilleure sera la qualité de la clé de chiffrement.

**Quatorzième étape.** Cliquez sur  pour poursuivre la création de votre *volume standard*.

**TrueCrypt** créera un fichier nommé *Mon volume* dans le répertoire *Mes documents*, tel que spécifié plus tôt. Ce fichier contiendra un *volume TrueCrypt standard*, d'une taille de 10 Mo, que vous pourrez utiliser pour stocker vos fichiers de façon sécurisée.

Quand la création du *volume standard* sera achevée, cette boîte de dialogue apparaîtra :

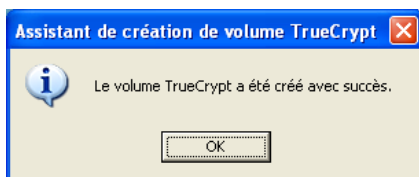
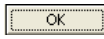


Figure 14: La boîte de dialogue *Le volume TrueCrypt a été créé avec succès*

**Quinzième étape.** Cliquez sur  pour finaliser la création du *volume standard* et revenir à la console **TrueCrypt**.

**Seizième étape.** Cliquez sur  pour fermer l'*Assistant de création de volume TrueCrypt*.

## Comment monter un volume standard

Sommaire des sections de cette page:

- [3.0 Comment monter un volume standard](#)
- [3.1 Comment démonter un volume standard](#)

---

### 3.0 Comment monter un volume standard

Dans **TrueCrypt**, *monter un volume* désigne le processus par lequel le volume est rendu accessible et prêt à l'utilisation. Dans cette section, vous apprendrez à *monter* le *volume standard* que vous venez de créer.

Pour entamer le montage du volume standard, suivez les étapes énumérées ci-dessous :

**Première étape.** Double-cliquez sur  ou Sélectionnez Démarrer > Programmes > TrueCrypt > TrueCrypt pour ouvrir TrueCrypt.

**Deuxième étape.** Sélectionnez un lecteur dans la liste, comme suit :

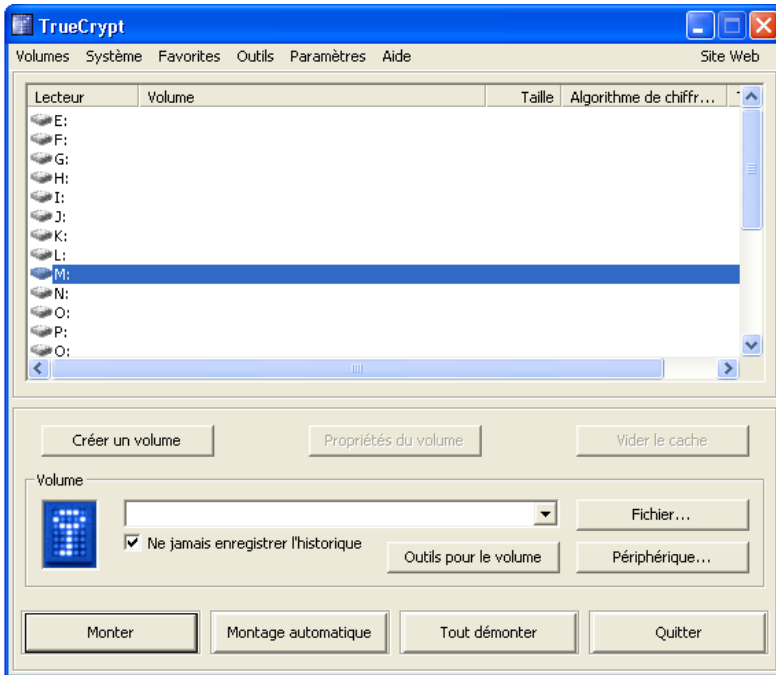


Figure 1: La console TrueCrypt

Dans cet exemple, le volume standard sera monté sur le lecteur M.

**Commentaire:** Dans la figure 1, le lecteur 'M' est sélectionné pour le montage du volume standard, mais vous pouvez choisir n'importe quel lecteur.

**Troisième étape.** Cliquez sur 

La fenêtre Sélectionner un volume TrueCrypt apparaîtra:

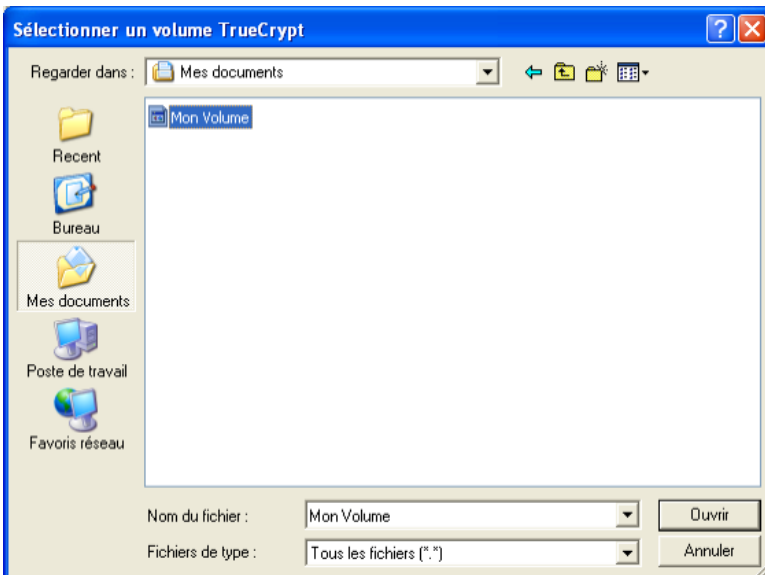




Figure 2: La fenêtre Sélectionner un volume TrueCrypt

**Quatrième étape.** Sélectionnez le fichier du volume standard que vous avez créé, puis cliquez sur  pour fermer la figure 2 et revenir à la console TrueCrypt.

**Cinquième étape.** Cliquez sur  pour activer la fenêtre Entrez le mot de passe pour..., illustrée ci-dessous:

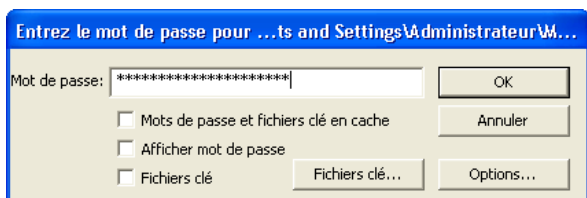



Figure 3: La fenêtre Entrez le mot de passe pour...

**Sixième étape.** Saisissez le mot de passe dans la zone de texte *Mot de passe*:

**Septième étape.** Cliquez sur  pour monter le *volume standard*.

**Commentaire:** Si le mot de passe que vous avez saisi est incorrect, **TrueCrypt** vous en avisera et vous devrez saisir le mot de passe de nouveau, puis cliquer sur . Si ce fois-ci le mot de passe est correct, le volume standard sera monté:

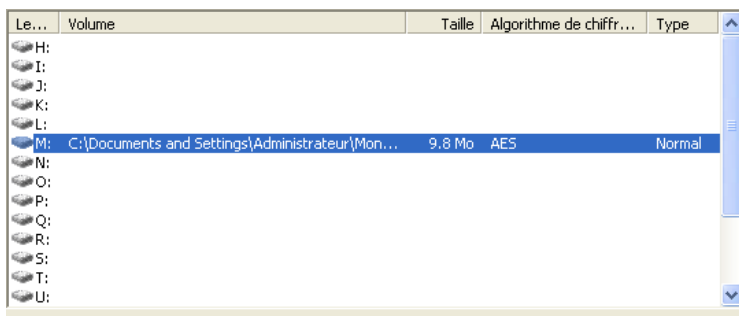


Figure 4: La console TrueCrypt affichant le volume standard nouvellement monté

**Huitième étape.** Double-cliquez sélection surlignée dans la liste **TrueCrypt** ou double-cliquez la lettre du disque correspondant dans la fenêtre *Poste de travail* pour accéder directement au *volume standard* maintenant monté sur le lecteur 'M:'.

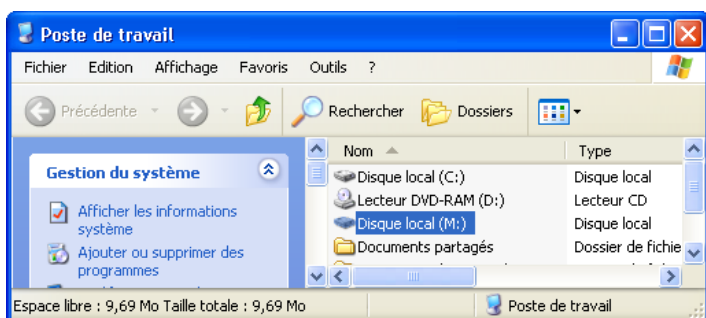


Figure 5: Accéder au volume standard via la fenêtre Poste de travail

**Commentaire:** Nous venons de monter le volume standard *Mon volume* en tant que lecteur virtuel *M:*. Ce lecteur virtuel a tous les attributs d'un vrai lecteur, sauf qu'il est complètement chiffré. Tous les fichiers copiés, déplacés ou sauvegardés dans ce disque virtuel seront automatiquement chiffrés (un processus appelé chiffrement à la volée).

Vous pouvez copier des fichiers dans le *volume standard*, exactement de la même façon qu'avec un lecteur normal (par exemple en le glissant depuis un autre répertoire). Lorsque vous déplacez un fichier depuis le *volume standard* vers un autre emplacement, celui-ci est automatiquement déchiffré. De la même façon, lorsque vous déplacez un fichier vers le *volume standard*, celui-ci est automatiquement chiffré. Lorsque votre ordinateur plante, ou s'il est soudainement éteint, **TrueCrypt** ferme automatiquement le *volume standard*.

**Important:** Après avoir transféré des fichiers dans le volume **TrueCrypt**, assurez-vous de ne laisser aucune trace de ces fichiers ailleurs sur l'ordinateur ou la clé USB dont ils proviennent. Veuillez consulter le chapitre **6. Détruire définitivement des données sensibles** <sup>[37]</sup> du livret pratique.

### 3.1 Comment démonter un volume standard

Dans **TrueCrypt**, le terme *démonter* désigne simplement le processus par lequel le volume est rendu inaccessible.

Pour fermer, ou démonter, un *volume standard* et faire en sorte que les fichiers qui s'y trouvent ne soient accessibles qu'aux personnes disposant du bon mot de passe, suivez les étapes énumérées ci-dessous :

**Première étape.** Sélectionnez le volume voulu dans la liste des volumes montés de la fenêtre principale de **TrueCrypt**:

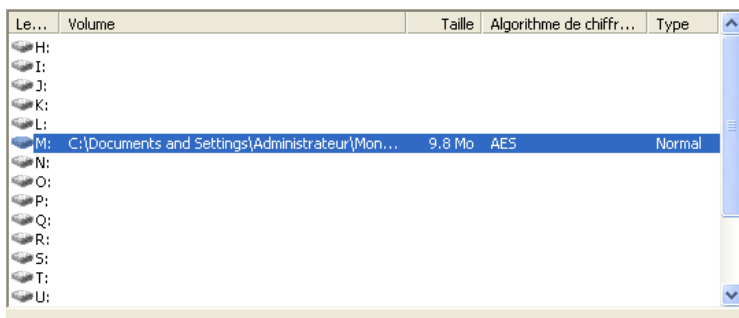



Figure 17: Sélectionner le volume standard à démonter

Deuxième étape. Cliquez sur  pour démonter, ou fermer, le *volume standard TrueCrypt*.

**Important:** Assurez-vous de démonter votre volume **TrueCrypt** avant de mettre l'ordinateur en *veille* ou en *veille prolongée*. En fait, il est plutôt conseillé d'éteindre le système complètement si vous avez l'intention de vous en éloigner. Cela empêchera tout intrus éventuel d'accéder au mot de passe de votre volume.

Pour récupérer les fichiers stockés dans votre volume standard, vous devrez monter le volume de nouveau.

## Comment créer des copies de sauvegarde de vos volumes

Il est très important de créer régulièrement des copies de sauvegarde de vos documents, fichiers et répertoires. La copie de sauvegarde de votre *volume TrueCrypt standard* est essentielle et (heureusement) facile à réaliser. N'oubliez pas de démonter votre volume avant d'en faire une copie de sauvegarde.

**Première étape.** Naviguez jusqu'au fichier qui contient votre *volume standard* (dans la *figure 1*, ci-dessous, ce fichier se trouve dans le répertoire *Mes Documents*).

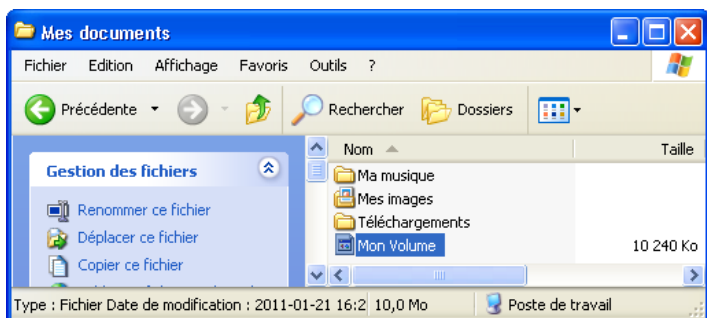


Figure 1: La recherche du fichier *Mon Volume*, dans la fenêtre *Mes documents*

**Deuxième étape.** Sauvegardez le fichier sur un support ou un dispositif de stockage amovible, comme un CD, un DVD ou une clé USB.

**Astuce:** Si vous avez une grande quantité de données que vous souhaitez chiffrer et archiver régulièrement, pourquoi ne pas créer un nouveau *volume standard* de la taille d'un CD ou d'un DVD? Cela peut être une technique d'archivage pratique et sécuritaire.

Avant de sauvegarder votre *volume standard* sur un support ou un dispositif amovible, assurez-vous que sa capacité de stockage correspond à la taille du volume.

Support de sauvegarde	Taille de volume TrueCrypt suggérée
CD	700 mo
DVD	3 900 mo
Clé USB	25% de la capacité de stockage totale (par ex. pour une clé USB de 128 Mo, utilisez 30 Mo pour votre volume standard)

## Volumes cachés

Sommaire des sections de cette page:

- [5.0 À propos des volumes cachés](#)
- [5.1 Comment créer un volume caché](#)
- [5.2 Comment monter un volume caché](#)
- [5.3 Conseils sur l'utilisation sécuritaire de la fonction disque caché](#)

### 5.0 À propos des volumes cachés


Dans **TrueCrypt**, un *volume caché* est placé à l'intérieur de votre *volume standard* chiffré, mais son existence est dissimulée. Même si vous *montez* votre volume standard, il est impossible de trouver un volume caché, ou même d'en prouver l'existence. Dans l'éventualité où l'on vous forcerait à révéler votre mot de passe et l'emplacement de votre volume standard, le contenu de ce dernier serait révélé, mais l'existence du volume caché resterait occultée.


Imaginez une valise pourvue d'un double fond. Les dossiers de peu d'importance, dont la perte ou la confiscation ne vous dérange pas, sont conservés dans le compartiment normal, mais les dossiers importants et privés sont dissimulés dans le double fond. L'intérêt d'un compartiment secret (surtout s'il est bien conçu) est justement le secret: toute personne hostile ou malveillante n'en perçoit tout simplement pas l'existence. **TrueCrypt** utilise cette technique à votre avantage.

## 5.1 Comment créer un volume caché

La création d'un *volume caché* est semblable à celle d'un *volume standard*. Certains panneaux et fenêtres ont exactement la même apparence.

**Première étape.** Ouvrez TrueCrypt.

**Deuxième étape.** Cliquez sur  pour afficher l'Assistant de création de volume de TrueCrypt.

**Troisième étape.** Cliquez sur  pour accepter l'option par défaut *Create an encrypted file container*.

**Quatrième étape.** Cochez l'option *Volume TrueCrypt caché*, comme suit:

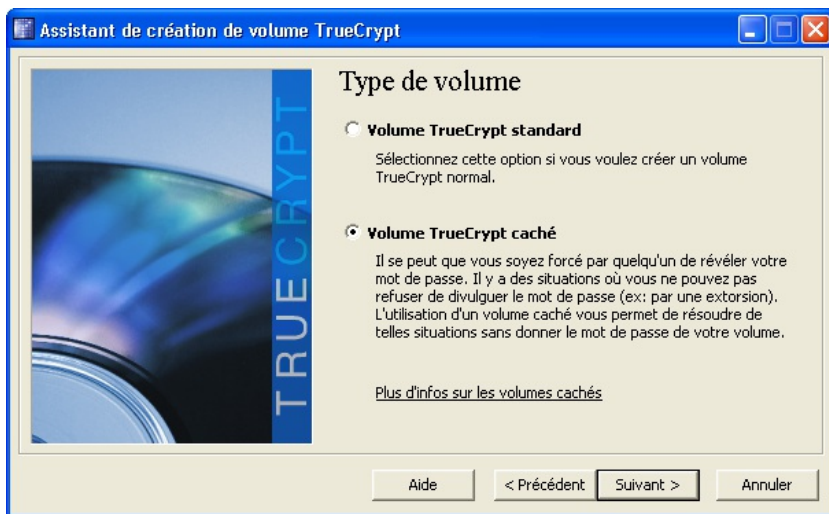


Figure 1: L'Assistant de création de volume TrueCrypt avec l'option *Volume TrueCrypt caché* sélectionné

**Cinquième étape.** Cliquez sur  pour afficher la fenêtre suivante:




Figure 2: La fenêtre *Mode création de volume*

- *Mode direct*: Cette option vous permet de créer un volume caché dans un *volume standard* existant.
- *Mode normal*: Cette option vous permet de créer un nouveau *volume standard*, à l'intérieur duquel vous incorporerez un *volume caché*.

Pour les fins de cet exercice, **cochez** l'option *Mode direct*.

**Commentaire:** Si vous souhaitez plutôt créer un nouveau *volume standard*, répétez les étapes détaillées à la section **2.2 Comment créer un volume standard** [83].

**Sixième étape.** Cochez l'option *Mode direct*, puis cliquez sur  pour afficher la fenêtre *Sélectionner un volume*

TrueCrypt.

**Commentaire:** Assurez-vous que le *volume standard* est démonté lorsque vous le sélectionnez.

**Septième étape.** Cliquez sur  pour afficher la fenêtre suivante:

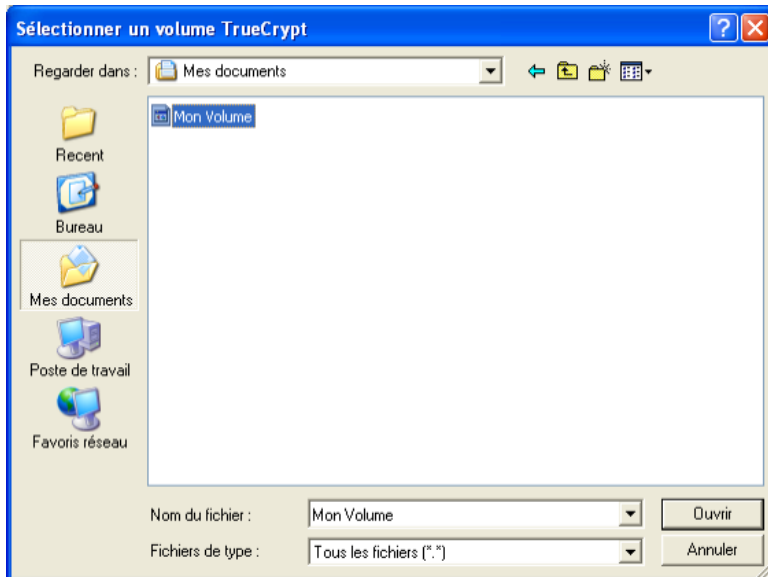


Figure 3: La fenêtre Sélectionner un volume TrueCrypt

**Huitième étape.** Trouvez le fichier du volume à l'aide de la fenêtre *Sélectionner un volume TrueCrypt*, tel qu'illustré à la figure 3.

**Neuvième étape.** Cliquez sur  pour revenir à l'*Assistant de création de volume*.

**Dixième étape.** Cliquez sur  pour afficher la fenêtre *Mot de passe du volume*.

**Onzième étape.** Saisissez le mot de passe que vous avez utilisé lors de la création du *volume standard* dans la zone de texte *Mot de passe* pour afficher la fenêtre suivante:

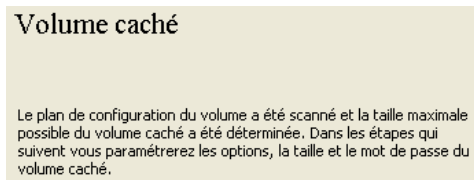


Figure 4: Le panneau volume caché

**Douzième étape.** Cliquez sur  après avoir lu le message pour afficher la fenêtre *Options de chiffrement du volume caché*.

**Commentaire:** Laissez les options de l'*Algorithme de chiffrement* et l'*Algorithme de hachage* du *\*volume caché\** telles quelles.

**Treizième étape.** Cliquez sur  pour afficher la fenêtre suivante:

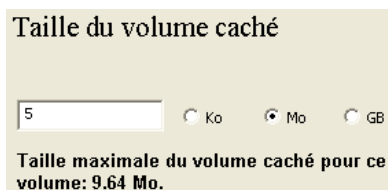


Figure 5: La fenêtre Taille du volume caché

Il faut maintenant choisir la taille du *volume caché*.

**Commentaire:** Tenez compte du type de documents, de leur taille ainsi que de la quantité de fichiers à stocker. N'oubliez pas de laisser de l'espace pour le *volume TrueCrypt standard*. Si vous choisissez la taille maximale disponible pour votre *volume caché*, vous ne pourrez plus stocker de fichiers dans le *volume standard* original.

Si votre *volume standard* est de 10 Mo et que vous indiquez que votre volume caché doit avoir 5 Mo (tel qu'illustré à la figure 5, ci-dessus), vous aurez deux volumes (un standard et l'autre caché) d'approximativement 5 Mo chacun.

Dans ce cas, vous devez vous assurer que les données que vous stockerez dans le *volume standard* ne dépassent pas 5 Mo. Le programme **TrueCrypt** ne détecte pas automatiquement l'existence d'un *volume caché* (par mesure de sécurité) et il est donc possible que les données qui s'y trouvent soient écrasées par mégarde. Vous risquez de perdre les données contenues dans le volume caché si vous dépassez la taille que vous aviez fixée.

**Quatorzième étape.** Saisissez la taille que vous souhaitez pour votre *volume caché* dans la zone appropriée de la fenêtre illustrée à la *figure 5*.

**Quinzième étape.** Cliquez sur  pour afficher la fenêtre *Mot de passe du volume caché*.

Vous devez maintenant choisir pour votre *volume caché* un mot de passe *différent* de celui que vous avez attribué au *volume standard*. N'oubliez pas de choisir un mot de passe fort. Pour plus d'information sur la création de mot de passes forts, voir le Guide pratique [KeePass](#) [82]. Vous devez absolument choisir un mot de passe différent de celui utilisé pour le *volume standard*.

**Astuce:** Si vous craignez qu'advienne une situation où vous êtes forcé de révéler le contenu de vos *volumes TrueCrypt*, archivez le mot de passe du *volume standard* dans **KeePass**, puis créez un mot de passe fort que vous mémoriserez pour le *volume caché*. Cela contribuera à protéger davantage le *volume caché*, puisque vous ne laisserez aucune trace de son existence.

**Seizième étape.** Créez un mot de passe, saisissez-le deux fois, puis cliquez sur  pour afficher la fenêtre suivante:

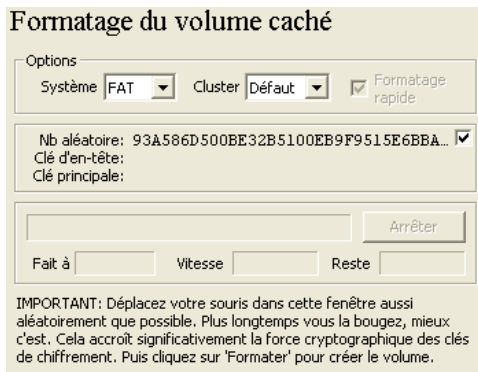


Figure 6: La fenêtre *Formatage du volume caché*

Laissez les options *Système* et *Cluster* telles qu'elles.

**Dix-septième étape.** Bougez la souris au dessus de la fenêtre pour accroître la force de chiffrement, puis cliquez sur  pour formater le *volume caché*.

Lorsque le formatage du *volume caché* est complété, vous verrez apparaître une fenêtre semblable à celle-ci:

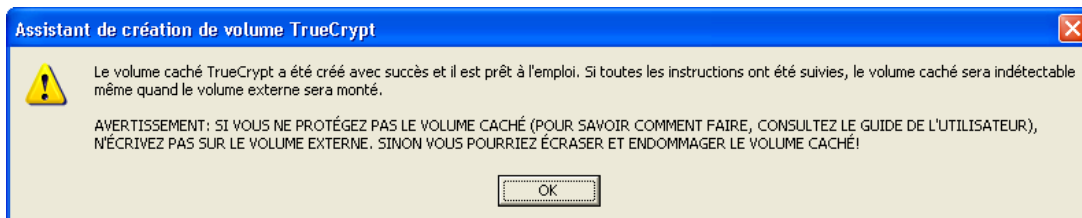


Figure 7: Fenêtre d'avertissement de l'Assistant de création de volume

**Commentaire:** La *Figure 7* ci-dessus confirme que vous avez bien créé un *volume caché* et vous rappelle le risque d'écraser des fichiers dans le *volume caché* lorsque vous stockez des fichiers dans le *volume standard* original.

**Dix-huitième étape.** Cliquez sur  pour afficher la fenêtre *Volume caché créé*, puis cliquez sur  pour revenir à la console **TrueCrypt**.

Le *volume caché* a été créé à l'intérieur de votre *volume standard*. Cela vous permet de cacher des documents à l'intérieur de votre *volume standard*. Ceux-ci resteront invisibles, même pour une personne qui a réussi à obtenir le mot de passe de ce *volume standard*.

## 5.2 Comment monter un volume caché

La méthode pour accéder à un *volume caché* est exactement de la même que pour un *volume standard*. La seule différence est que vous devez utiliser le mot de passe du *volume caché* plutôt que celui du *volume standard*. C'est par le mot de passe que **TrueCrypt** détermine s'il doit ouvrir le *volume standard* ou le *volume caché*.

Pour *monter*, ou ouvrir, le *volume caché*, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez un lecteur dans la liste (dans cet exemple, le lecteur K):




Figure 8: Un lecteur sélectionné dans la fenêtre des volumes de **TrueCrypt**

**Deuxième étape.** Cliquez sur  pour afficher la fenêtre *Sélectionnez un volume TrueCrypt*.



**Troisième étape.** Naviguez jusqu'à votre fichier de volume **TrueCrypt** (le même fichier que pour votre *volume standard*), puis **sélectionnez-le**.

**Quatrième étape.** Cliquez sur  pour revenir à la console **TrueCrypt**.

**Cinquième étape.** Cliquez sur  pour afficher la fenêtre *Entrez le mot de passe pour...*, tel qu'illustré ci-dessous:

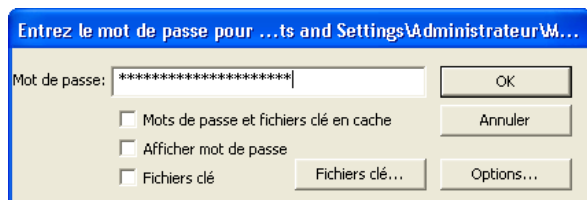


Figure 9: La fenêtre *Entrez le mot de passe pour...*

**Sixième étape.** Saisissez le mot de passe que vous avez choisi lors de la création du *volume caché*, puis **cliquez** sur



Le *volume caché* est maintenant monté (ouvert), tel qu'illustré ci-dessous:

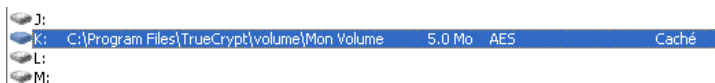


Figure 10: La fenêtre principale de TrueCrypt affichant le *volume caché* récemment monté

**Septième étape.** Double-cliquez sur cette entrée ou passer par la fenêtre *Poste de travail*.

## 5.3 Conseils sur l'utilisation sécuritaire de la fonction disque caché

Le but de la fonction lecteur caché est de vous soustraire à toute situation potentiellement dangereuse en *laissant l'impression* à un adversaire que vous lui donnez ce qu'il veut - l'accès à vos fichiers - sans pour autant compromettre la sécurité de vos données. En plus de protéger vos données, cela vous permet d'éviter de vous mettre davantage en danger ou d'exposer vos collègues et partenaires. Pour que cette technique soit efficace, vous devez créer une situation où votre adversaire sera satisfait des résultats de sa recherche et cessera de vous importuner.

Pour que cela soit efficace, vous devriez suivre ces quelques indications:

- Placez vos documents semi-sensibles, ceux dont la perte vous dérange moins, dans le *volume standard*. Ces documents doivent tout de même être assez "intéressants" pour capter l'attention de votre adversaire lorsque vous serez forcé de les lui montrer.
- Gardez à l'esprit que votre adversaire est peut être conscient de la possibilité de créer des *volumes cachés* avec **TrueCrypt**. Cela dit, si vous utilisez **TrueCrypt** correctement, cette personne ne sera pas en mesure de prouver l'existence d'un volume caché, ce qui rendra votre démenti plus crédible.
- Actualisez régulièrement (une fois par semaine) les fichiers placés dans le *volume standard*. Cela donnera l'impression que vous utilisez réellement ces fichiers.

Lorsque vous montez un volume **TrueCrypt**, il vous est toujours possible d'activer la fonction *Empêcher les dommages causés en écrivant dans le volume externe*. C'est une option extrêmement importante qui vous permet d'ajouter des fichiers de "diversion" à votre *volume standard* sans devoir vous inquiéter de supprimer ou d'écraser le contenu chiffré de votre *volume caché*.

Comme nous l'avons déjà vu, il existe un risque que vous écrasiez vos fichiers cachés lorsque vous dépassez la limite d'espace que vous avez déterminée pour votre *volume standard*. Vous ne devriez jamais activer l'option *Protection du volume caché* lorsque vous êtes forcé par quelqu'un de monter un volume **TrueCrypt**, parce que vous seriez alors obligé de saisir le mot de passe secret de votre *volume caché* et cela révélerait automatiquement l'existence dudit volume. Lorsque vous actualisez vos fichiers de "diversion" en privé, par contre, vous devriez *toujours* activer cette option.

Pour utiliser l'option *Protection du volume caché*, suivez les étapes énumérées ci-dessous.

**Première étape.** Cliquez sur  de la fenêtre *Entrez le mot de passe pour...* illustrée à la figure 9, ci-dessus, pour afficher la fenêtre *Options de montage*, illustrée ci-dessous:

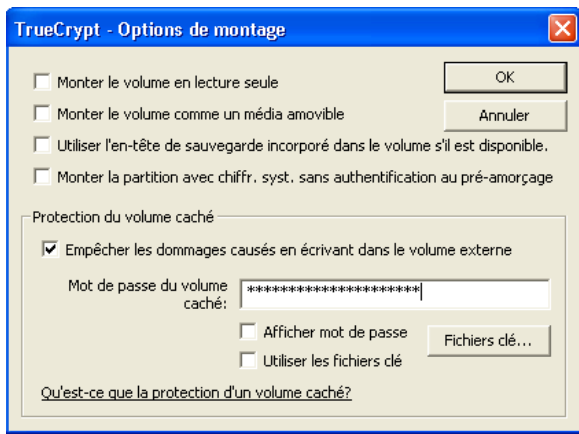





Figure 11: La fenêtre Options de montage

**Deuxième étape.** Cochez l'option *Empêcher les dommages causés en écrivant dans le volume externe*.

**Troisième étape.** Saisissez le mot de passe de votre *volume caché*, puis cliquez sur .

**Quatrième étape.** Cliquez sur  pour monter votre *volume standard*. Lorsque celui-ci sera monté, vous serez en mesure d'ajouter des fichiers de "diversion" sans endommager les fichiers stockés dans votre *volume caché*.

**Cinquième étape.** Cliquez sur  pour démonter votre *volume standard* quand vous avez fini d'en actualiser le contenu.

**N'oubliez pas:** Vous ne devez effectuer cette opération que lorsque vous actualisez les fichiers qui se trouvent dans votre *volume standard*. Lorsque vous révélez l'existence de votre volume standard à quelqu'un, vous ne devriez pas utiliser la fonction *Protection du volume caché*.

## Faq et questions récapitulatives

### 6.0 Faq et questions récapitulatives

Claudia et Pablo sont satisfaits de ce que leur offre **TrueCrypt**, d'autant plus que le programme est facile à installer et fonctionne maintenant automatiquement. Cependant, avant de décider définitivement de l'utiliser, ils ont encore quelques questions à propos de **TrueCrypt**.

**Q:** Est-ce que je vais devoir passer tout mon temps à saisir des mots de passe?

**A:** Non, tu n'auras qu'à saisir ton mot de passe une seule fois, à l'ouverture du volume standard. Lorsque cela est fait, tu peux ouvrir tous les fichiers contenu dans le volume sans devoir saisir de mots de passe.

**Q:** Puis-je désinstaller **TrueCrypt** facilement si je n'en veux plus? Si je désinstalle le programme, mes fichiers seront-ils toujours chiffrés?

**A:** Oui, on peut facilement désinstaller **TrueCrypt** en sélectionnant **Démarrer > Programmes > Truecrypt > Uninstall Truecrypt**.

Cependant, tu dois retirer tous tes fichiers du volume standard avant de désinstaller le programme, sinon il ne te sera plus possible d'y accéder, à moins de réinstaller **TrueCrypt** ou de transférer le fichier du volume standard sur un ordinateur où est installé le programme. Si tu transfères ton volume standard sur un autre ordinateur, tu auras toujours besoin du bon mot de passe pour y accéder.

**Q:** Si j'ai un problème avec **TrueCrypt**, y a-t-il une adresse de courriel ou un site Internet où je peux trouver de l'aide?

**A:** Pour obtenir du soutien technique, consulte la documentation en ligne sur le site de **TrueCrypt** <http://www.TrueCrypt.org/docs/> [80] ou sur le forum à <http://forums.truecrypt.org/> [84], ou encore sur le site Internet Security Box [http://security.ngoinabox.org/fr/truecrypt\\_principale](http://security.ngoinabox.org/fr/truecrypt_principale) [85]. Cela dit, personne ne pourra retrouver un mot de passe oublié!

**Q:** Est-ce que différentes versions de **Windows** affichent différents formats de fenêtre lorsqu'on utilise **TrueCrypt**?

**A:** L'apparence des fenêtres peut varier un peu, mais le contenu est toujours le même.

**Q:** Quels types de fichiers doit-on chiffrer?

**A:** Idéalement, tu devrais chiffrer tous tes documents, images ou fichiers qui contiennent des renseignements privés ou sensibles. S'il advenait que ton ordinateur soit perdu ou confisqué, l'information comprise dans ton volume **TrueCrypt** serait à l'abri.

**Q:** Dans quelle mesure nos fichiers seront-ils sécurisés?

**A:** **TrueCrypt** a été testé de façon indépendante par des spécialistes de la sécurité informatique pour évaluer sa performance et déterminer si toutes les fonctions incluses dans le programme opèrent tel qu'annoncé. Les résultats de ces examens révèlent que **TrueCrypt** est un excellent programme, qui offre un niveau élevé de protection. Le choix d'un mot de passe fort est essentiel pour préserver la sécurité de vos volumes.

La fonction de volume caché de *TrueCrypt* présente un niveau de sécurité exceptionnel pour les données stockées sur votre ordinateur. L'utilisateur doit avoir une excellente maîtrise du programme et de ses fonctions de base, ainsi qu'une bonne compréhension de ses propres risques en terme de sécurité et des situations où la fonction de volume caché peut s'avérer utile.

**Q:** Est-il possible d'endommager ou détruire le disque caché par inadvertance?

**A:** Oui. Si vous continuez d'ajouter des fichiers au volume standard jusqu'à ce qu'il n'y ait plus assez d'espace (pour que le volume caché puisse exister), votre volume caché sera automatiquement écrasé. Il existe une option dans le menu de *TrueCrypt* qui sert à protéger votre volume caché contre l'écrasement ou la suppression accidentelle, mais l'utilisation de cette fonctionnalité peut révéler l'existence d'un volume caché.

**Q:** Puis-je modifier la taille de mon volume caché après l'avoir créé?

**A:** Non. Il vous faudra créer un autre volume caché et y transférer vos fichiers manuellement.

**Q:** Puis-je utiliser 'chkdsk', 'Défragmenteur de disque', ou d'autres outils semblables sur un volume monté *TrueCrypt*?

**A:** Les volumes *TrueCrypt* se comportent exactement comme de vrais disques. Il est donc possible d'utiliser n'importe quel outil de vérification, de réparation ou de défragmentation du contenu sur un volume *TrueCrypt*.

**Q:** Est-il possible de changer le mot de passe d'un volume caché?

**A:** Oui. La fonction 'Modifier le mot de passe du volume' s'applique aussi bien aux volumes cachés qu'aux volumes standards. Vous n'avez qu'à saisir le mot de passe actuel du volume caché dans la zone de texte 'Mot de passe actuel' de la fenêtre de l'option 'Modifier le mot de passe du volume'.

**Q:** Quand devrais-je utiliser la fonction de volume caché?

**A:** Utilisez la fonction de volume caché de *TrueCrypt* lorsque vous devez dissimuler l'existence de certains renseignements se trouvant sur votre ordinateur. Notez bien que cela est différent de l'utilisation d'un volume standard, qui sert essentiellement à protéger l'accès à vos renseignements.

Pour une foire aux questions détaillée à propos de *TrueCrypt*, <http://www.TrueCrypt.org/faq.php> <sup>[86]</sup>

## 6.1 Questions récapitulatives portant sur les volumes standards

- Qu'est-ce que le chiffrement?
- Qu'est-ce qu'un *volume standard*?
- Comment peut-on créer un *volume standard* sur une clé USB?
- Quels sont les différentes façon de démonter un *volume standard*?
- Comment peut-on choisir et conserver un bon mot de passe pour protéger un *volume standard*?
- Quelles sont les options pour la création d'une copie de sauvegarde de votre *volume standard*?
- Décrivez quelques une des méthodes utilisées pour dissimuler la présence du *volume standard* sur votre ordinateur.

## 6.2 Questions récapitulatives portant sur les volumes cachés

- Quel est la principale différence entre un *volume standard* et un *volume caché*?
- Quel types de fichiers devraient être placés dans un *volume standard* si vous utilisez aussi un *volume caché*?
- Où est situé le *volume caché*?
- Quel est la taille idéale d'un *volume caché*?
- Quels sont les avantages et désavantages associés à l'option qui protège votre *volume caché* contre une suppression ou un écrasement accidentel?

# Cobian - copies de sauvegarde

**Cobian Backup** sert à créer des copies de sauvegarde ou des « archives » de vos fichiers et répertoires. Les copies de sauvegarde peuvent être stockées dans d'autres répertoires ou lecteurs de votre ordinateur, sur les autres ordinateurs d'un réseau de travail ou sur des supports amovibles.

### Site Internet

[www.educ.umu.se/~cobian/cobianbackup.htm](http://www.educ.umu.se/~cobian/cobianbackup.htm)  
<sup>[87]</sup>

### Configuration requise :

- Windows NT/2000/XP/Vista (version 8)
- Windows 95, 98, ME sont compatibles avec la [version 7](#) <sup>[88]</sup> de Cobian Backup

### Version utilisée pour rédiger ce guide :

- 8.4.0.202

### Pour installer Cobian

- Lisez la courte introduction des [Guides pratiques](#) <sup>[89]</sup>
- Cliquez sur l'icône ci-dessous et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Lisez attentivement la 'Notice d'installation' avant de continuer.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.



#### Licence :

- Gratuitiel (*Freeware*)

#### Lecture préalable :

- Livret pratique Security in-a-box, chapitre 5. [Récupérer des données perdues](#) [91].

**Niveau :** 1 : Débutant, 2 : Moyen, 3 : **intermédiaire**, 4 : Expérimenté, 5 : Avancé

**Temps d'apprentissage :** 30 minutes

#### Ce que vous apportera l'utilisation de cet outil :

- La capacité de créer des copies de sauvegarde pour tous vos documents, fichiers et répertoires.
- La capacité de compresser et décompresser vos fichiers de sauvegarde.
- La capacité de chiffrer et déchiffrer vos fichiers archivés.

### 1.1 À propos de cet outil

Cobian Backup sert à créer des copies de sauvegarde ou des "archives" de vos fichiers et répertoires. Les copies de sauvegarde peuvent être stockées dans d'autres répertoires ou lecteurs de votre ordinateur, sur les autres ordinateurs d'un réseau de travail ou sur des supports amovibles (CD, DVD et clés USB). Vous pouvez planifier le moment où des copies de sauvegarde de fichiers et de répertoires devront être créées. Le programme peut rouler en arrière-plan de votre système (c'est-à-dire dans la barre des tâches de votre système), consulter votre horaire et générer des copies de sauvegarde lorsque cela est nécessaire. Cobian Backup peut également compresser et chiffrer des fichiers en même temps qu'il crée les copies de sauvegarde.

### 1.2 Commentaire sur l'installation

Durant le processus d'installation, vous devrez régler une série d'options. Nous recommandons de **cocher** l'option *en tant que service* pour vous assurer que le programme soit actif en tout temps (en arrière-plan) et que vos copies de sauvegarde soient créées automatiquement en temps voulu.

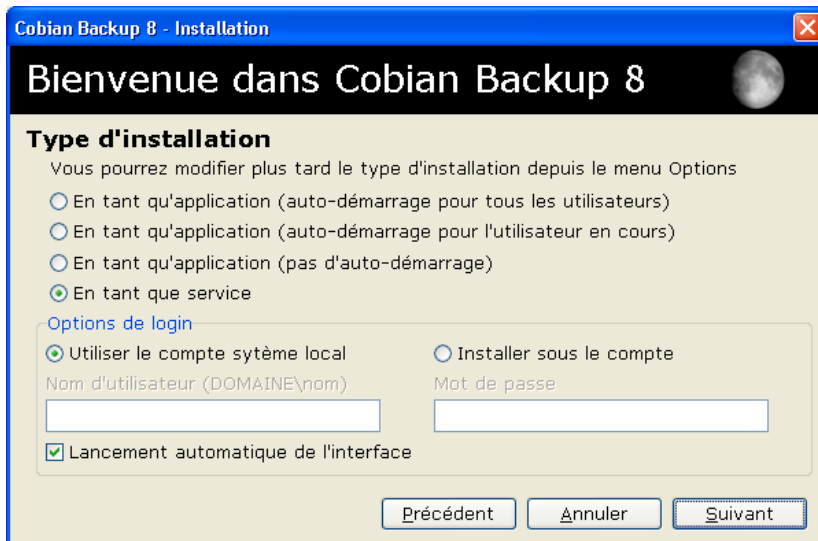


Figure 1 : La fenêtre d'installation de Cobian Backup 8

#### Offline Installation Instructions :

##### Pour installer Cobian Backup

- \*Lisez la courte **Introduction** aux **Guides pratiques** [1]\*\*
- **Cliquez sur l'icône Cobian Backup ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.

#### Cobian Backup:



## Créer une copie de sauvegarde

Cette section aborde les configurations minimales nécessaires à la création de copies de sauvegarde de groupes de fichiers. D'autres sections aborderont la compression et/ou le chiffrage des copies de sauvegarde des fichiers. **Cobian**

**Backup** vous permet de créer des tâches de sauvegarde qui peuvent être configurées pour inclure un groupe particulier de fichiers et/ou de répertoires. Vous pouvez régler le programme pour que ces tâches de sauvegarde soient exécutées à des heures et des jours déterminés.

Pour créer une tâche de sauvegarde, suivez les étapes énumérées ci-dessous :



**Première étape.** Cliquez sur : pour créer une nouvelle tâche de sauvegarde.

Ceci active la fenêtre *Propriétés de*:

Le menu de gauche vous offre d'activer les différentes fenêtres et d'établir les paramètres nécessaires à la procédure de sauvegarde.

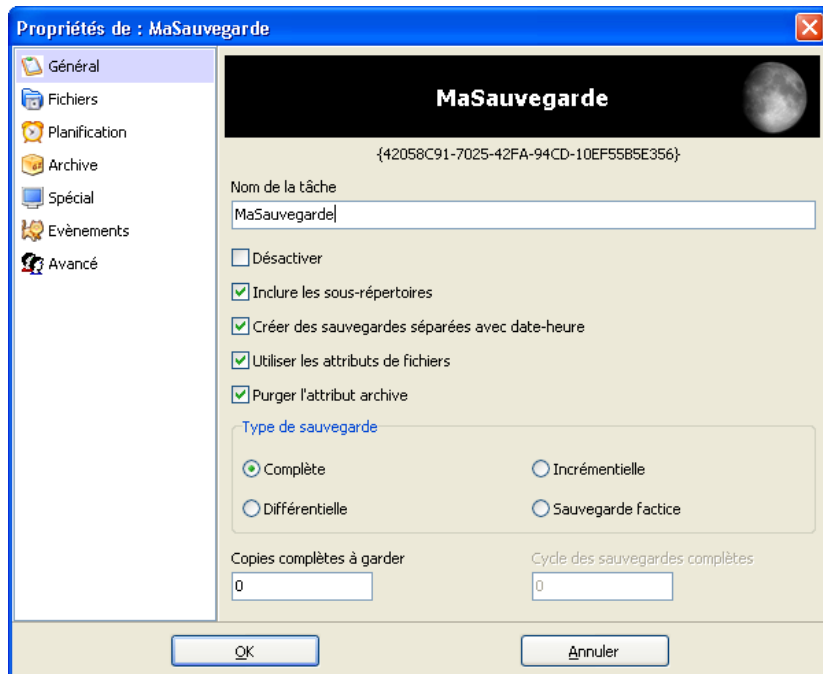


Figure 2 : La fenêtre *Propriétés de*: affichant le nom du fichier *MaSauvegarde* nouvellement créé

## 2.1 Description des options

**Nom de la tâche** : Sélectionnez un nom pour la tâche. Utilisez un nom qui désigne la nature de la copie de sauvegarde. Par exemple, si la copie de sauvegarde contiendra les fichiers vidéo, vous pouvez la nommer *Copie de sauvegarde vidéo*.

**Désactiver** : Laissez la case *désactiver* non cochée. **Avertissement** : Si vous cochez cette option, la tâche ne s'exécutera pas.

**Inclure les sous-répertoires** : Si cette option est cochée, tout dossier qui se trouve dans le dossier que vous avez sélectionné sera inclus. Cette méthode est efficace pour créer des copies de sauvegarde d'un grand nombre de fichiers. Par exemple : si vous sélectionnez le dossier *Mes documents* et cochez cette option, tous les fichiers et dossiers dans *Mes documents* seront inclus dans la copie de sauvegarde.

**Créer des copies de sauvegarde séparées avec date-heure** : Cette option signifie qu'une fois la copie de sauvegarde terminée, l'heure et la date à laquelle elle a été créée apparaîtra dans le nom du dossier qui contient la copie de sauvegarde. Cette option est intéressante parce qu'elle vous permettra de reconnaître facilement le moment où la copie de sauvegarde a été créée.

**Utiliser les attributs de fichiers** : Cette option n'est utile que si vous choisissez de créer une copie de sauvegarde incrémentielle ou différentielle (voir détails ci-dessous). Les attributs de fichiers contiennent de l'information au sujet du fichier.

Cobian Backup vérifie cette information afin de déterminer si un changement a été apporté au fichier source depuis la dernière fois qu'une copie de sauvegarde a été créée. Si vous exécutez une copie de sauvegarde incrémentielle ou différentielle, le fichier sera mis à jour. **Commentaire** : Vous ne serez en mesure d'exécuter une copie de sauvegarde complète ou "factice" que si vous décochez cette option (la copie de sauvegarde "factice" est expliquée ci-dessous).

## 2.2 Description des types de copies de sauvegarde

**Complète** : Tous les fichiers se trouvant à l'emplacement source seront copiés dans votre répertoire de copies de sauvegarde. Si vous cochez l'option *Créer des copies de sauvegarde séparées avec date-heure*, vous aurez plusieurs copies provenant de la même source (identifiées au moyen de l'heure et de la date, incluses dans le nom du fichier, où la copie a été créée). Autrement dit, le programme écrasera la version antérieure (s'il en existe une).

**Incrémentielle** : Le programme vérifiera si les fichiers source ont été modifiés depuis la création de la plus récente copie de sauvegarde. Le programme ignorera les fichiers qui n'ont pas besoin d'être copiés, ce qui économisera du temps. L'option *Utiliser les attributs de fichiers* doit être cochée pour que ce type de sauvegarde puisse être exécutée.

**Bit d'archive** : Il s'agit d'information sur la taille du fichier et sur la date de création et de modification. Cette information permet à Cobian Backup de déterminer si le fichier a été modifié par vous depuis la dernière création d'une copie de sauvegarde.

**Différentielle** : Le programme vérifiera si la source a été modifiée depuis la dernière création d'une copie de sauvegarde **complète**. Le programme ignorera les fichiers qui n'ont pas besoin d'être copiés, ce qui économisera du temps. Si vous avez auparavant exécuté une copie de sauvegarde complète du même groupe de fichiers, vous pouvez alors continuer à créer des copies de sauvegarde en utilisant la méthode différentielle.

**Sauvegarde factice** : Cette option correspond à une fonction de copie de sauvegarde dont nous n'avons pas vraiment besoin. Tu peux l'utiliser pour que ton ordinateur exécute ou ferme certains programmes à des moments précis. Cette option, de niveau avancé, est peu utile à nos procédures de copie de sauvegarde.

## 2.3 Comment créer un fichier de sauvegarde

Pour démarrer la création d'un fichier de sauvegarde, suivez les étapes énumérées ci-dessous :

**Première étape.** Cliquez sur l'icône *Fichiers* dans le coin gauche de la fenêtre *Propriétés de* : pour sélectionner les fichiers qui seront copiés.

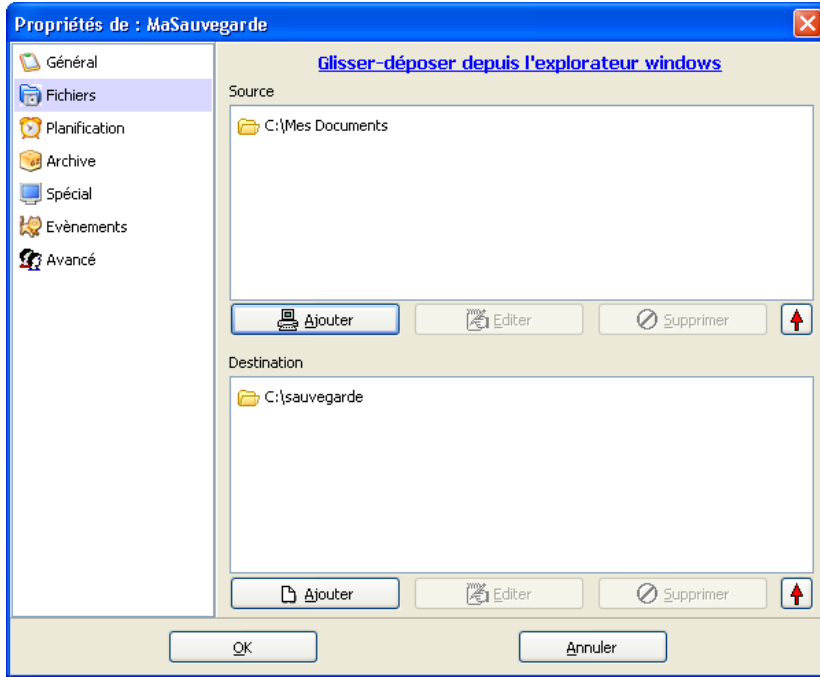


Figure 3 : La fenêtre *Propriétés de* : affichant les fenêtres *Source* et *Destination*

**Deuxième étape.** Sélectionnez les fichiers que vous souhaitez copier. (Dans l'exemple précédent, le dossier *Mes documents* est sélectionné.)

**Troisième étape.** Cliquez sur  dans la fenêtre **Source** pour activer le menu suivant :



Figure 4 : La fenêtre *Source* – le menu du bouton *Ajouter*

**Quatrième étape.** Sélectionnez *Fichiers* pour créer des copies de sauvegarde de fichiers individuels, et *Répertoire* si vous souhaitez créer une copie de sauvegarde d'un répertoire entier ou pour indiquer quel fichier ou répertoire doit être copié.

**Commentaire** : Vous pouvez ajouter autant de fichiers ou de répertoires que vous le souhaitez. Si vous souhaitez effectuer une sauvegarde de fichiers se trouvant déjà sur votre serveur FTP, **sélectionnez** l'option *Site FTP* (vous aurez besoins des détails de connexion appropriés pour vous connecter au serveur).

Après avoir sélectionné les fichiers et/ou dossiers, vous les verrez apparaître dans la zone *Source*. Comme vous le constatez avec l'exemple ci-dessous, *Mes documents* est affiché dans cette partie, ce qui veut dire que ce dossier fait maintenant partie de la copie de sauvegarde.

La fenêtre *Destination* désigne l'endroit où les copies de sauvegarde seront stockées.

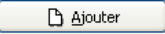
**Cinquième étape.** Cliquez sur :  dans la fenêtre *Destination* pour activer le menu suivant :



Figure 5 : La fenêtre *Destination* – le menu du bouton *Ajouter*

**Sixième étape.** Sélectionnez *Répertoire*. Une fenêtre de navigation s'ouvre par laquelle vous devez sélectionner le répertoire de destination de votre copie de sauvegarde.

**Commentaire :** Si vous souhaitez créer différentes versions de la copie de sauvegarde du fichier, vous pouvez à ce moment sélectionner plusieurs répertoires. Si vous avez coché l'option *Manuellement*, vous devez saisir le chemin complet vers le répertoire où vous souhaitez conserver la copie de sauvegarde. Pour utiliser un serveur Internet distant pour stocker votre archive, **sélectionnez** l'option *Site FTP* (vous aurez besoins des détails de connexion appropriés pour vous connecter au serveur).

La fenêtre devrait maintenant ressembler à l'exemple ci-dessus, avec des fichiers et/ou des répertoires dans la zone source et des répertoires dans la zone destination. Toutefois, ne cliquez pas tout de suite sur *OK*! Nous devons encore planifier la création de nos copies de sauvegarde!

## 2.4 Comment planifier vos tâches de sauvegarde

La dernière partie que nous devons aborder afin que nos copies de sauvegarde automatiques soient fonctionnelles est la partie *Planification*. Cette partie vous permet de déterminer les moments où vous souhaitez que vos copies de sauvegarde soient créées.

Pour régler les options de planification, suivez les étapes énumérées ci-dessous :

**Première étape. Sélectionnez *Planification***, dans le menu de gauche, pour activer la fenêtre suivante :

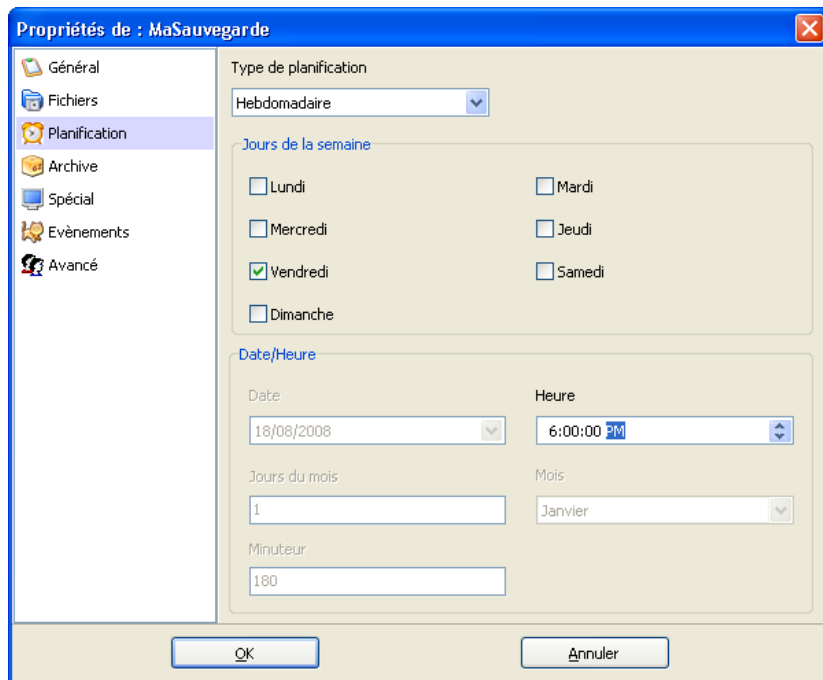


Figure 6 : Les Propriétés de MaSauvegarde affichant la fenêtre *Type de planification*.

Les options de *Type de planification* sont énumérées dans un menu défilant. Elles sont décrites ci-dessous :

*Une fois* : La copie de sauvegarde sera créée une seule fois à la date et à l'heure que vous inscrivez dans la zone *Date/Heure*.

*Quotidienne* : La copie de sauvegarde sera créée chaque jour à la date et à l'heure que vous inscrivez dans la zone *Date/Heure*.

*Hebdomadaire* : La copie de sauvegarde sera créée le jour de la semaine que vous aurez choisi. Dans l'exemple ci-dessus, la copie est créée le vendredi. Vous pouvez aussi choisir une autre journée. La copie de sauvegarde sera créée selon les journées et l'heure inscrites dans la zone *Date/Heure*.

*Mensuelle* : La copie de sauvegarde sera créée selon les journées choisies dans la boîte *mois* à l'heure inscrite dans la zone *Date/Heure*.

*Annuelle* : La copie de sauvegarde sera créée selon les journées choisies dans la boîte *mois*, au cours du mois que vous aurez également choisi et à l'heure inscrite dans la zone *Date/Heure*.

*Minuterie* : La copie de sauvegarde sera créée à plusieurs reprises aux intervalles inscrits dans la boîte *Minuteur* de la zone *Date/Heure*.

*Manuellement* : Vous devrez exécuter la copie vous-même depuis la fenêtre principale du programme.

**Deuxième étape. Cliquez** sur le bouton *OK*.

La *planification des sauvegardes clôt le processus*. Des copies de sauvegarde des fichiers sélectionnés seront désormais créées aux moments que vous avez déterminés.

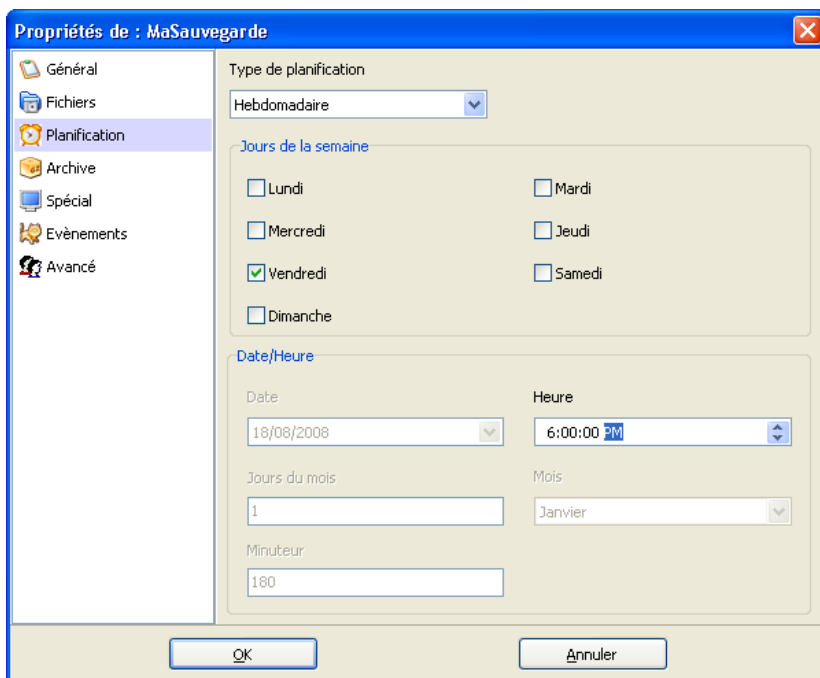


Figure 7 : Les propriétés de MaSauvegarde affichant le panneau Type de planification

## Compresser vos archives

**Étape 1.** Créez une tâche de sauvegarde pour tous les fichiers que vous souhaitez archiver en suivant les étapes énumérées à la section **2.3 Créer une copie de sauvegarde** [93].

**Étape 2.** Sélectionnez l'option *Archive* dans le menu de gauche pour activer la fenêtre *Propriétés de*:

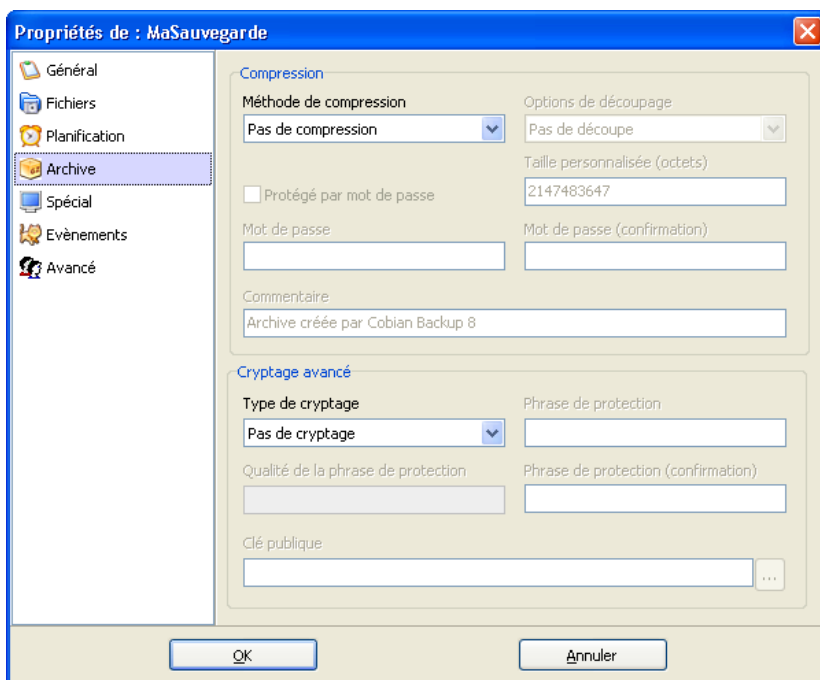


Figure 8 : La fenêtre Propriétés de: affichant les rubriques Compression et Cryptage avancé

### 3.1 Comment compresser vos archives

La rubrique *Compression* sert à déterminer la méthode de compression de votre choix.

La compression sert à réduire l'espace employé pour stocker vos fichiers. Supposons que votre ordinateur contienne une série de vieux fichiers dont vous ne servez plus, mais que vous souhaitez tout de même conserver. Il est logique que vous les stockiez dans un format qui occupe le moins d'espace possible en ayant recours aux techniques de compression et de décompression. La compression enlève les éléments de codification peu importants d'un document, tout en conservant l'information importante. La compression n'abîme pas vos données originales. Les fichiers ne sont pas visibles lorsque compressés. Le processus inverse, la *décompression*, doit être appliqué aux fichiers pour les rendre visibles à nouveau.

Les trois sous-options du menu défilant de la *méthode de compression* sont :

*Pas de compression* : Tel que son nom l'indique, cette option n'exécute pas de compression.



**Compression Zip** : Il s'agit de la technique de compression normale pour les systèmes **Windows**. Les archives, une fois créées, peuvent être ouvertes à l'aide des outils Windows habituels (vous pouvez aussi télécharger le programme [ZipGenius](#) [94] pour les ouvrir). Cette option est la plus pratique des trois.

**Compression SQX** : La compression SQX est plus lente que la compression Zip. Cependant, en cas de corruption des archives, son taux de récupération des données est plus élevé.

Si vous avez choisi l'une des trois options de compression mentionnées ci-dessus, vous pouvez également choisir :

**Options de découpage**, du menu défilant. Cette option est pratique pour stocker des données sur des supports portatifs comme des CD, des DVD, des disquettes ou des clés USB. Vos archives seront découpées en morceaux dont la taille correspond au dispositif de stockage de votre choix. Supposons que vous copiez un grand nombre de fichiers, que vous souhaitez les transférer sur un CD et que la taille de vos archives dépasse 700 Mo (la taille d'un CD). La fonction de découpage divisera vos archives en morceaux plus petits que 700 Mo, ou équivalents à cette taille : vous pourrez alors les graver sur un ou plusieurs CD. Si vous prévoyez créer des copies de sauvegarde du disque dur de votre ordinateur ou que la taille de votre copie de sauvegarde est inférieure à la capacité de stockage de votre dispositif, vous pouvez passer cette section.

Les options de taille suivantes vous sont offertes lorsque vous cliquez sur le menu défilant **Options de découpage**. Votre choix dépendra du dispositif de stockage que vous souhaitez utiliser.

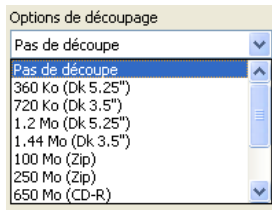


Figure 9 : Le menu défilant **Options de découpage**

- 3,5" – Disquette. Cette option contient assez d'espace pour y stocker un petit nombre de documents.
- Zip – Disque Zip (vérifiez la capacité du disque Zip que vous utilisez). Vous aurez besoin d'un lecteur de disque Zip connecté à votre ordinateur et des disques personnalisés.
- Disque CD-R – CD (vérifiez la capacité du disque que vous utilisez). Vous aurez besoin d'un graveur de CD connecté à votre ordinateur et d'un programme d'écriture de CD.
- Disque DVD – DVD (vérifiez la capacité du disque que vous utilisez). Vous aurez besoin d'un graveur DVD connecté à votre ordinateur et d'un programme d'écriture DVD.

Si vous créez des copies de sauvegarde que vous stockez sur plusieurs clés USB, vous avez peut-être intérêt à fixer une taille personnalisée.

Pour ce faire, suivez les étapes énumérées ci-dessous :

**Première étape.** Sélectionnez l'option *Taille personnalisée*, et saisissez la taille de l'archive en octets dans la zone de texte :

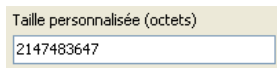


Figure 10 : La zone de texte **Taille personnalisée**

Un aperçu des tailles :

- 1 Ko (kilooctet) = 1 024 octets – un document texte d'une page fait à l'aide de Open Office correspond environ à 20 Ko.
- 1 Mo (mégaoctet) = 1 024 Ko – une photo prise à l'aide d'une caméra numérique se situe généralement entre 1 et 3 Mo.
- 1 Go (gigaoctet) = 1 024 Mo – environ une demi-heure d'un film DVD de bonne qualité.

**Commentaire** : Lorsque vous choisissez une taille personnalisée pour découper vos copies de sauvegarde afin de les stocker sur un DVD ou un CD, Cobian Backup ne copiera pas automatiquement la sauvegarde sur votre dispositif de stockage. Le programme créera plutôt vos archives sur votre ordinateur, et vous devrez les graver vous-même sur le CD ou le DVD.

**Protéger par mot de passe** : Cette option vous permet de choisir un mot de passe pour protéger vos archives. Saisissez simplement, deux fois, un mot de passe dans les zones de texte appropriées. Au moment de décompresser l'archive, le programme vous demandera votre mot de passe avant d'exécuter la tâche.

**Commentaire** : Si vous souhaitez augmenter le niveau de sécurité de l'archive, vous devriez envisager d'utiliser une autre méthode que celle du mot de passe. Cobian Backup vous permet également de chiffrer votre archive. Cette méthode sera abordée dans la section qui suit, **4. Chiffrer vos archives** [95]. Sinon, vous pouvez aussi consulter le [Guide pratique TrueCrypt](#) [96] pour apprendre comment créer un volume de stockage chiffré sur votre ordinateur ou sur un dispositif amovible.

**Commentaire** : Cette option vous permet d'inscrire une information descriptive au sujet de l'archive (facultatif).

### 3.2 Comment décompresser votre archive

Pour décompresser votre archive, suivez les étapes énumérées ci-dessous :

**Première étape.** Sélectionnez : **Outils > Décompacteur**

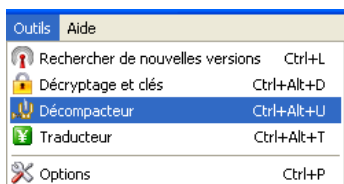


Figure 16 : Le menu Outils affichant l'option Décompacteur

La fenêtre *Décompacteur* apparaît :

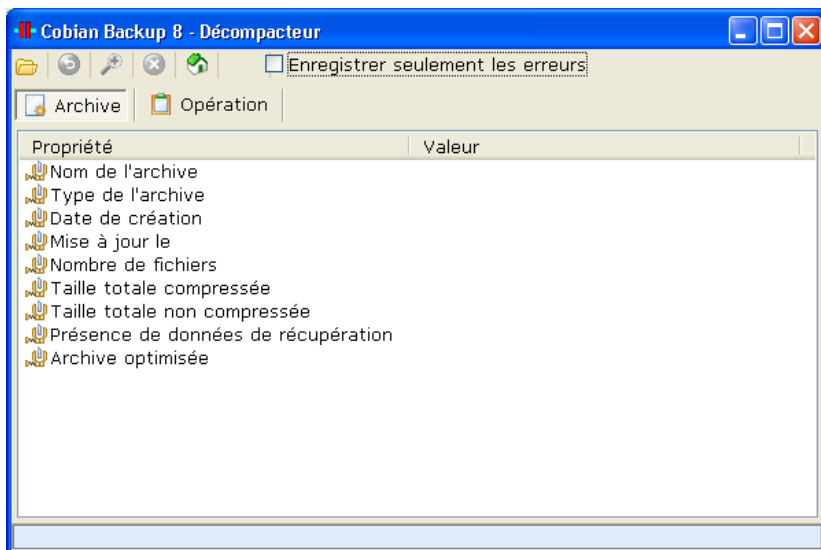



Figure 17 : La fenêtre Cobian Backup - Décompacteur

**Deuxième étape.** Cliquez sur : 

**Troisième étape.** Sélectionnez l'archive (fichier .zip ou .sqx)

**Quatrième étape.** Cliquez sur le bouton *OK*.

**Cinquième étape.** Sélectionnez un répertoire où vous souhaitez décompresser le fichier archivé.

**Sixième étape.** Cliquez sur : 

Vous verrez apparaître une nouvelle fenêtre qui vous permettra de choisir le répertoire où vous souhaitez décompresser l'archive.

**Septième étape.** Sélectionnez un répertoire.

**Huitième étape.** Cliquez sur le bouton *OK*.

Utilisez **Windows Explorer** pour voir les fichiers transférés dans ce répertoire.

## Chiffrer vos archives

Le chiffrement peut s'avérer nécessaire si vous voulez protéger vos copies de sauvegarde des accès non autorisés. Le *Chiffrement* est le processus de codification, ou d'embrouillage, des données : une fois chiffrées, les données sont inintelligibles pour quiconque ne détient pas la clé nécessaire au décodage du message. Pour plus de renseignements sur le chiffrement, veuillez consulter le chapitre [4. Protéger les données sensibles stockées sur votre ordinateur](#) <sup>[97]</sup> du livret pratique.

### 4.1 Comment chiffrer vos archives

La fenêtre *Cryptage avancé* sert à préciser la méthode de chiffrement que vous souhaitez utiliser.

**Étape 1 :** Cliquez sur le menu défilant *Type de cryptage* pour activer la liste des diverses méthodes de chiffrement :

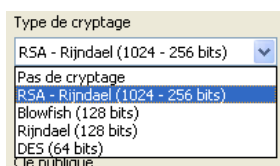


Figure 11 : Le menu défilant des types de chiffrement

Par souci de simplicité, nous vous recommandons de choisir entre les méthodes *Blowfish* et *Rijndael* (128 octets). Ces méthodes sont très sûres et vous permettent d'accéder aux données chiffrées à l'aide d'une phrase de protection que vous choisirez.

**Deuxième étape :** Sélectionnez le *type de chiffrement* de votre choix.

**Commentaire :** *Rijndael* et *Blowfish* s'équivalent en ce qui concerne le niveau de sécurité. *DES* est plus faible, mais le processus de chiffrement est plus rapide.

**Troisième étape :** Saisissez (deux fois) la phrase de protection dans les boîtes appropriées, tel que dans l'exemple suivant :

Type de cryptage	Phrase de protection
Blowfish (128 bits)	*****
Qualité de la phrase de protection	Phrase de protection (confirmation)
	*****

Figure 12 : Les zones de texte du *Type de chiffrement* et de la *phrase de protection*

La force de la phrase de protection est indiquée par la barre *Qualité de la phrase de protection*. Plus la barre bouge vers la droite, plus la phrase de protection est forte. Voir le chapitre 3. Créer et sauvegarder des mots de passe sûrs du livret pratique pour obtenir des directives sur la création et le stockage de mots de passe sûrs.

**Quatrième étape :** Cliquez sur le bouton *OK*.

## 4.2 Comment déchiffrer votre archive

**Étape 2. Sélectionnez :** Outils > Décryptage et clés

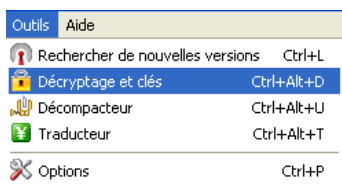


Figure 13 : Le menu *Outils* avec l'option *Décryptage et Clés* sélectionnée

Ceci activera la fenêtre *Décryptage et clés* :

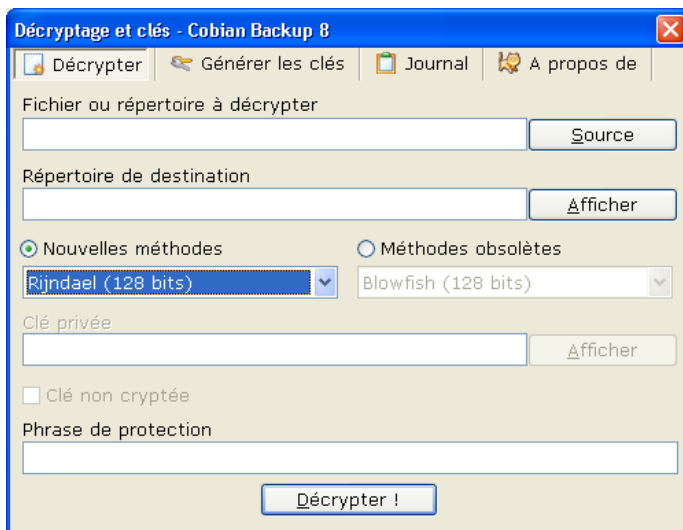


Figure 14 : La fenêtre *Décryptage et Clés* dans *Cobian Backup 8*

**Deuxième étape.** Cliquez sur le bouton *Source* pour sélectionner l'archive que vous souhaitez déchiffrer.

**Troisième étape.** Cliquez sur le bouton *Afficher* pour sélectionner le répertoire où l'archive doit être stockée.

**Quatrième étape.** Sélectionnez le type de chiffrement (que vous avez choisi à la section 4.1 **Comment chiffrer vos archives**) dans le menu défilant *Nouvelles méthodes*.

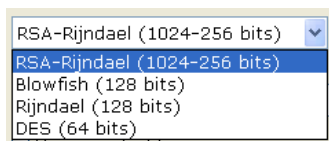


Figure 15 : Le menu défilant *Nouvelles méthodes*

**Cinquième étape.** Sélectionnez la méthode de chiffrement appropriée (celle que vous avez utilisée pour chiffrer votre copie de sauvegarde).

**Sixième étape.** Saisissez votre *Phrase de protection* dans la zone de texte du même nom.

**Septième étape.** Cliquez sur le bouton *Décrypter*.

Les fichiers seront déchiffrés vers l'emplacement que vous avez spécifié. Si les fichiers étaient également compressés, vous devrez les décompresser en suivant les étapes énumérées à la section **3.2 Comment décompresser vos archives**.

[98]

## Faq et questions récapitulatives

Elena et Nikolai savent à quel point il est important de créer des copies de sauvegarde de leurs documents : ils ont déjà perdu des fichiers importants suite au bris d'un ordinateur causé par un virus. **Cobian Backup** est une solution adéquate au problème de rationalisation du processus de création de copies de sauvegarde, bien que l'on doive prendre un peu de temps pour l'installer et s'y habituer.

Elena, après avoir appris à s'en servir, est heureuse d'utiliser la fonction de base de création de copies de sauvegarde. Elle sait qu'elle peut conserver ses copies dans un emplacement sûr, loin de son ordinateur et de son bureau. De plus, elle trouve que la fonction de compression des fichiers de sauvegarde est très utile puisqu'elle permet d'économiser de l'espace sur son ordinateur. Nikolai est particulièrement content de pouvoir utiliser un seul programme pour à la fois chiffrer un document d'archive et en créer une copie de sauvegarde. Il est aussi intéressé à approfondir l'option *Sauvegarder sur un serveur distant par ftp* dans un avenir rapproché, afin de pouvoir stocker des copies de fichiers importants sur des serveurs qui se trouvent ailleurs dans le monde.

Toutefois, Elena et Nikolai ont tous deux quelques questions au sujet de Cobian Backup :

**Q.** : *Si je conserve les archives de mes fichiers sur un DVD, est-ce que je peux décompresser et déchiffrer mes fichiers sur un autre ordinateur que le mien? Est-ce possible de les utiliser dans un café Internet?*

**R.** : *Tu peux restaurer ton archive, qu'elle soit chiffrée ou compressée, sur n'importe quel ordinateur où Cobian Backup est installé.*

**Q.** : *Je suis aux prises avec un véritable problème d'espace sur mon ordinateur. J'ai des doutes quant à l'espace que je pourrai économiser en compressant mes fichiers. Peux-tu me donner quelques exemples simples?*

**R.** : *La majeure partie de l'espace d'un ordinateur est habituellement occupée par des fichiers photos, vidéo et audio. Tu peux vérifier l'espace que ces fichiers occupent sur ton ordinateur en cliquant à droite sur le répertoire qui les contient et en choisissant l'option Propriétés. Si tu as peu d'espace libre sur ton ordinateur, tu peux envisager de créer des archives des fichiers pour ensuite retirer les originaux de ton ordinateur.*

**Q.** : *On me demande toujours de mettre à jour des programmes que j'obtiens sur Internet. Si une nouvelle version de Cobian Backup est créée et que je la télécharge, j'ai peur de ne plus avoir accès à mes fichiers compressés et chiffrés. Devrais-je télécharger des mises à jour?*

**R.** : *Tu devrais toujours télécharger les plus récentes mises à jour, puisqu'elles apportent souvent des améliorations opérationnelles et sécuritaires. Cobian Backup continuera de bien fonctionner sur ton ordinateur, et toutes les nouvelles versions seront compatibles avec les copies créées avec une ancienne version du programme.*

**Q.** : *La présence de ce programme sur mon ordinateur ne signale-t-elle pas clairement que j'ai des données chiffrées?*

**R.** : *Tu n'as pas besoin de conserver une copie de sauvegarde chiffrée sur ton ordinateur. Cobian Backup n'est pas un programme réputé pour le chiffrement de données, puisque ce n'est pas sa fonction principale.*

**Q.** : *Est-ce préférable d'utiliser Cobian Backup ou TrueCrypt pour chiffrer des fichiers ?*

**R.** : *Il est préférable d'utiliser TrueCrypt pour chiffrer des fichiers sur ton ordinateur. Le mécanisme de chiffrement est plus puissant et offre la possibilité d'ajouter et de supprimer des fichiers du volume chiffré. Tu peux par ailleurs créer une copie de sauvegarde d'un volume TrueCrypt à l'aide de Cobian Backup.*

**Q.** : *Y a-t-il d'autre information que je dois connaître avant d'installer l'option de Sauvegarde sur serveur distant par FTP?*

**R.** : *Tu devrais savoir si ton fournisseur offre le service FTP, et connaître les détails d'ouverture de session. Il est préférable que tu utilises une version sécurisée de FTP, le SFTP, si cette option est offerte par ton fournisseur de service.*

### 4.1 Questions récapitulatives

1. Quelle est la différence entre les copies de sauvegarde incrémentielles et différentielles ?
2. Quelle est la meilleure façon de sécuriser une copie de sauvegarde?
3. Comment stocker une copie de 1 Go sur un disque CD?
4. Comment restaurer un seul fichier d'une copie de sauvegarde?
5. Est-il possible de créer une tâche automatisée de sorte que votre ordinateur mette à jour les copies de sauvegarde une fois par semaine, le vendredi après-midi? Quelles sont les étapes à suivre pour y arriver ?

## Recuva - récupération de fichiers

### Short Description:

**Recuva** est un outil facile à utiliser qui permet de récupérer des fichiers perdus. Vous pouvez scanner vos disques pour récupérer des documents, fichiers, dossiers ou autres données, y compris des messages de courrier électronique, des images et des clips vidéo. **Recuva** emploie également des techniques d'écrasement sécurisées pour effacer des données sensibles et/ou privées.

### Online Installation Instructions:

#### Pour installer Recuva

- Lisez la courte introduction des **Guides pratiques** <sup>[1]</sup>
- Cliquez sur l'icône **Recuva** ci-dessous pour afficher la page de téléchargement [www.piriform.com/recuva/builds](http://www.piriform.com/recuva/builds)
- Dans la section 'Recuva - Slim', cliquez sur le bouton 'Download'

- **Sauvegardez** le fichier exécutable 'rcsetup\_slim.exe' sur votre ordinateur, puis **double-cliquez** dessus pour lancer l'installation du programme
- Lisez attentivement les 'consignes d'installation' détaillées à la prochaine section avant de continuer
- Après avoir complété l'installation de **Recuva** vous pouvez supprimer l'exécutable d'installation de votre ordinateur

Recuva:



[99]

Site Internet

[www.piriform.com/recuva](http://www.piriform.com/recuva) [100]

Configuration requise

- Compatible avec toutes les versions de Windows (**Commentaire:** Le soutien technique pour **Windows 98** n'est plus disponible.)

Version utilisée pour rédiger ce guide

- 1.3

Licence

- Gratuitiel

Lecture requise

- Livret pratique Security in-a-box, chapitre **5. Récupérer des données perdues** [101]

Niveau: 1: Débutant, 2: **Moyen**, 3: Intermédiaire, 4: Expérimenté, 5: Avancé

Temps d'apprentissage: 20 minutes

Ce que vous apportera l'utilisation de cet outil:

- La capacité d'exécuter différentes méthodes de scan
- La capacité de récupérer des fichiers préalablement supprimés de votre ordinateur
- La capacité d'effacer de façon sécurisée certaines données privées ou sensibles

Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

Pour les utilisateurs **GNU Linux**, nous recommandons **R-Linux** [102].

Les utilisateurs de **Mac OS** apprécieront sans doute **TestDisk** et **PhotoRec** [103], qui sont également compatibles avec **Microsoft Windows** et **GNU Linux**.

À part **Recuva**, il existe d'autres programmes de récupération de données compatibles avec **Microsoft Windows**:

- **NTFS Undelete** [104]
- **Disk Digger** [105]
- **PCInspector File Recovery** [106]
- **Undelete Plus** [107]

## 1.1 À propos de cet outil

Dans les situations fâcheuses où certaines données sensibles auraient pu être supprimées par accident, **Recuva** peut vous aider à les restaurer. Comme nous l'avons vu au chapitre **6. Détruire définitivement des données sensibles** [37], un fichier supprimé à l'aide de la méthode de suppression standard du système **Windows**, même après que la *corbeille* eut été vidée, existe peut-être toujours quelque part sur le disque dur.

Il existe tout de même certaines circonstances où **Recuva** n'est pas en mesure de retrouver les données. Si vous avez effacé, ou supprimé de façon permanente, des fichiers temporaires à l'aide de **CCleaner** et de sa fonction *Effacement sécurisé (Lent)*, ces fichiers sont irrécupérables. **Recuva** ne peut pas récupérer des fichiers après que des programmes comme **CCleaner** ou **Eraser** aient été utilisés pour effacer l'espace libre de vos disques durs, ou après que **Windows** ait écrasé lesdits fichiers avec de nouvelles données. De plus, **Recuva** ne peut pas récupérer des fichiers ou documents endommagés.

**Recuva** peut également être utilisé pour écraser de façon sécuritaire des données privées ou sensibles.

Offline Installation Instructions :

Pour installer Recuva

- \*Lisez la courte **Introduction** aux **Guides pratiques** [1]\*\*
- **Cliquez sur l'icône Recuva ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.

Recuva:



[108]

## Comment installer Recuva

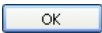
## 2.0 Comment installer Recuva

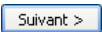
L'installation de **Recuva** est relativement simple et rapide. Pour lancer l'installation de **Recuva**, suivez les étapes énumérées ci-dessous:

**Première étape.** Double-cliquez sur  ; Il est possible que s'ouvre une boîte de dialogue *Fichier ouvert - Avertissement de sécurité*. Si c'est le cas, cliquez sur  pour afficher la boîte de dialogue suivante:



Figure 1: La boîte de sélection de la langue de l'assistant

**Deuxième étape.** Cliquez sur  pour afficher l'Assistant d'installation de **Recuva**.

**Troisième étape.** Cliquez sur  pour afficher la fenêtre *Licence utilisateur*. Veuillez lire attentivement la *Licence Utilisateur* avant de poursuivre le processus d'installation.

**Quatrième étape.** Cliquez sur .

**Cinquième étape.** Cliquez sur  pour afficher la fenêtre *Options d'installation*.

**Commentaire:** Selon la version, il est possible que la fenêtre *Options d'installation* s'affiche avec l'option *Install optional Yahoo! toolbar* sélectionnée par défaut. Si c'est le cas, désélectionnez cette option parce qu'elle pourrait compromettre votre confidentialité sur Internet. (NDT: Dans la version v1.38, cette option a été éliminée du processus d'installation.)

**Sixième étape.** Désélectionnez l'option *Install optional Yahoo! toolbar*.

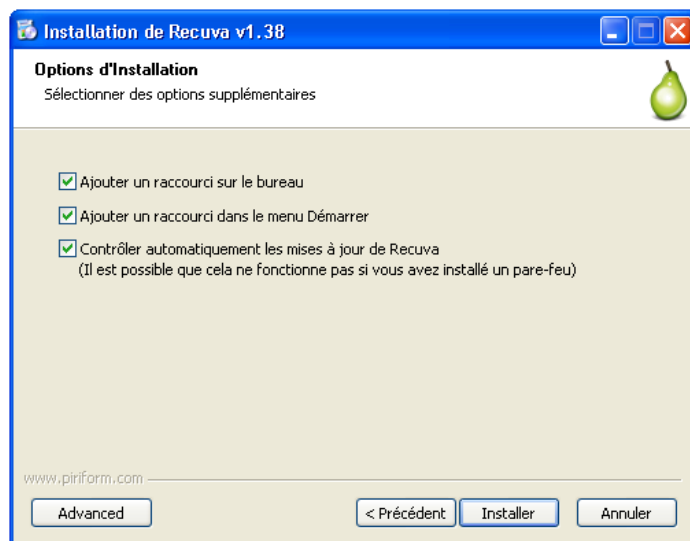
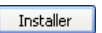


Figure 2: La fenêtre Options d'installation

**Septième étape.** Cliquez sur  pour lancer l'installation de **Recuva**. La barre de progression de l'installation s'affichera momentanément, puis l'installation se complètera d'elle-même en quelques minutes.

**Huitième étape.** \*Cliquez sur  pour finaliser l'installation de **Recuva**.

Maintenant que vous avez finalisé l'installation de **Recuva**, vous êtes prêt à récupérer et/ou écraser des données privées ou sensibles. Pour ce faire, veuillez lire attentivement la section [3.0 Comment exécuter différents types de scan avec Recuva](#) <sup>[109]</sup>.

## Comment exécuter différents types de scan avec Recuva

Sommaire des sections de cette page:

- [3.0 Avant de commencer](#)
- [3.1 Comment exécuter un scan avec l'assistant de Recuva](#)
- [3.2 Comment exécuter un scan sans utiliser l'assistant de Recuva](#)
- [3.3 Comment exécuter une Analyse approfondie avec Recuva](#)
- [3.4 Une introduction à la fenêtre Options](#)

### 3.0 Avant de commencer

Dans cette section, nous verrons comment lancer différents types de scans et nous examinerons les onglets *Général* et *Actions* de la fenêtre *Options*.

**Commentaire:** Un scan ne fait que retrouver et afficher les fichiers récupérables. Le processus de récupération comme tel sera examiné à la section **4.0 Comment récupérer et effacer des fichiers de façon sécuritaire avec Recuva** [110].

#### 3.1 Comment exécuter un scan avec l'assistant de Recuva

L'*Assistant* de **Recuva** est recommandé dans les situations où le nom du fichier à récupérer n'est pas connu. Ce mode est également recommandé si vous utilisez **Recuva** pour la première fois. L'*Assistant* de **Recuva** vous laisse régler les paramètres du scan en vous permettant de spécifier le type de fichier et/ou l'emplacement original du fichier supprimé.


Pour commencer à chercher les fichiers supprimés, suivez les étapes énumérées ci-dessous:

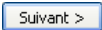


**Première étape.** Cliquez sur  ou sélectionnez **Démarrer > Programmes > Recuva > Recuva** pour lancer le programme et afficher la fenêtre suivante:



Figure 1: La fenêtre *Bienvenue dans l'assistant de Recuva*

**Astuce:** Si vous connaissez le nom du fichier que vous souhaitez récupérer, au complet ou en partie, cliquez sur  pour vous afficher l'interface principale de *Piriform Recuva*. Vous n'avez ensuite qu'à suivre les consignes décrites à la section **3.2 Comment exécuter un scan sans utiliser l'assistant de Recuva**.

**Deuxième étape.** Cliquez sur  pour afficher la fenêtre suivante:

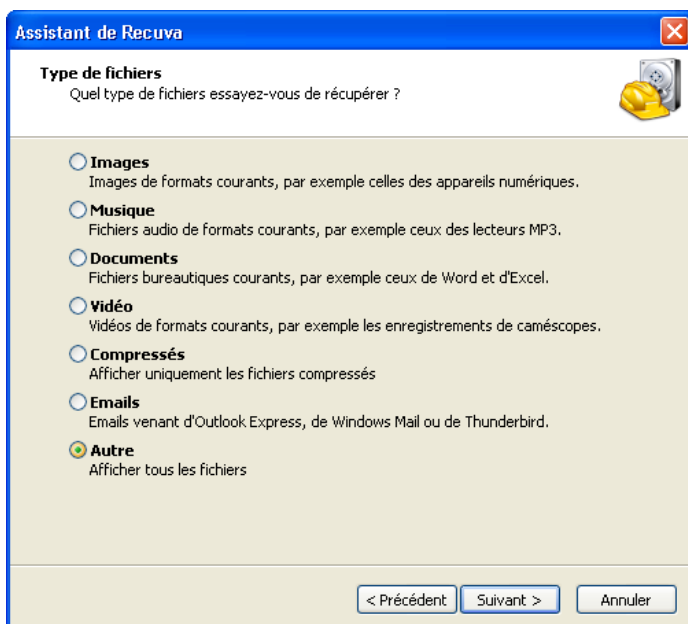



Figure 2: La fenêtre *Type de fichiers* de l'assistant de Recuva

La fenêtre *Type de fichiers* affiche une liste des différents types de fichiers et décrit quels fichiers peuvent être récupérés lorsque l'une ou l'autre des options est sélectionnée.

**Troisième étape.** Cochez l'option *autre*, tel qu'illustré à la *Figure 2*, puis cliquez sur  pour afficher la fenêtre suivante:

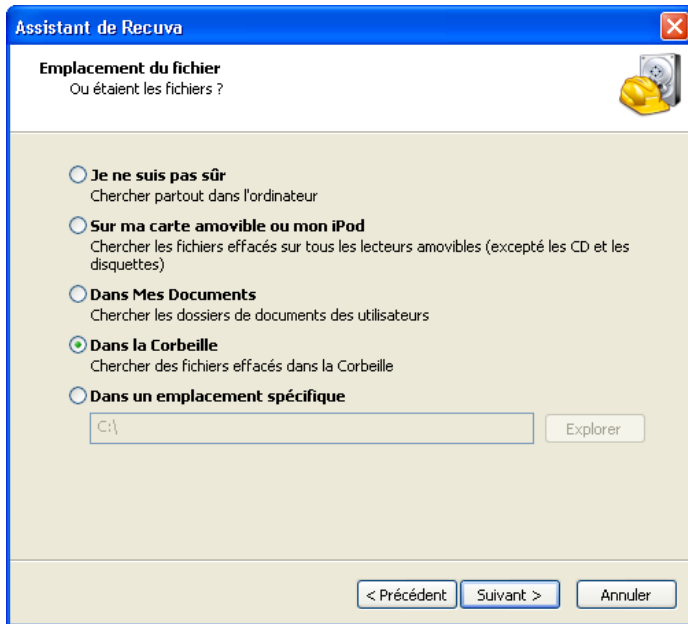


Figure 3: La fenêtre *Emplacement du fichier* de l'Assistant de Recuva

**Commentaire:** Le réglage par défaut de la fenêtre *Emplacement de fichier* est *Je ne suis pas sûr*. Cette option lancera un scan sur tous les disques et sur tous les dispositifs amovibles, à l'exception des CD, DVD et médias optiques. Il est donc possible qu'un tel scan prennent un certain temps à générer des résultats.

Le plus souvent, les fichiers sont supprimés à partir de la *Corbeille* du système d'exploitation *Windows*, pour réduire les chances que vous supprimiez des données sensibles ou privées.


**Quatrième étape.** Cochez l'option *Dans la corbeille*, tel qu'illustré à la *Figure 3* ci-dessus, puis cliquez sur  pour afficher la fenêtre suivante:



Figure 4: *Merci, maintenant Recuva est prêt à chercher vos fichiers*

**Commentaire:** Pour les fins de cet exercice, n'activez pas l'option *Analyse approfondie*. Cette technique de scan sera abordée à la section **3.3 Comment exécuter une analyse approfondie**.

**Première étape.** Cliquez sur  pour entamer la restauration de vos fichiers supprimés.

Au cours du processus de récupération, de barre de progression s'affichent successivement. La barre de progression *Recherche des fichiers effacés sur les lecteurs* liste les fichiers supprimés. La barre de progression *Analyse du contenu du fichier* regroupe et trie les fichiers supprimés par types de fichiers et selon qu'ils sont récupérables ou non. Elle affiche également la durée estimée du processus de scan et d'analyse. L'interface principale de *Piriform Recuva* ressemblera alors à ceci:



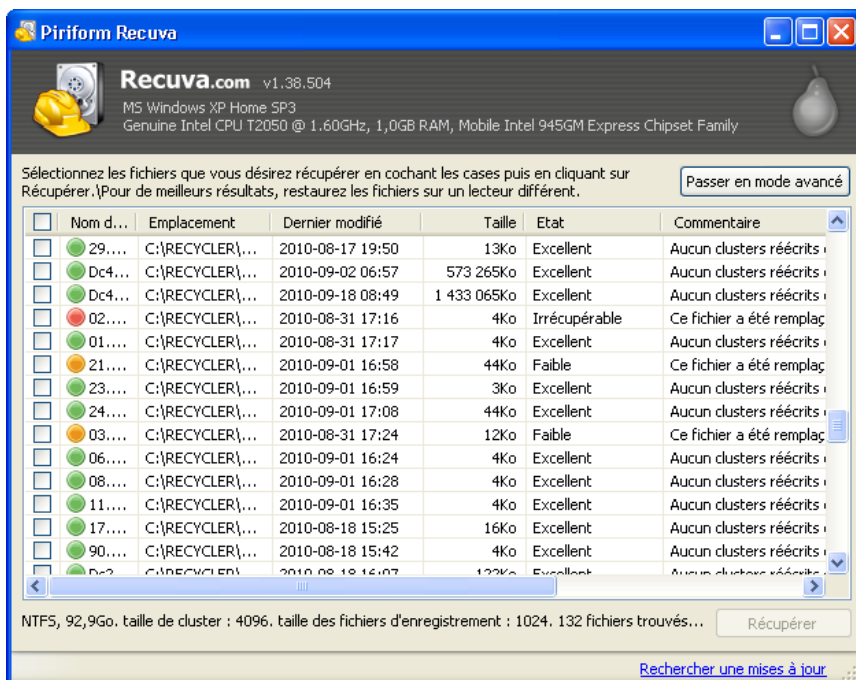


Figure 5: L'interface principale de Piriform Recuva affichant des fichiers supprimés retrouvés

L'interface principale de Piriform Recuva liste des renseignements sur chaque fichier supprimé en six colonnes. Voici une description de chaque colonne:

**Nom du fichier:** Cette colonne affiche le nom et l'extension de fichier du fichier supprimé. Cliquez sur le titre *Nom du fichier* pour arranger les résultats en ordre alphabétique.

**Emplacement:** Cette colonne affiche l'emplacement où le fichier a été retrouvé. Puisque l'option *Dans la corbeille* a été sélectionnée dans cet exemple, l'emplacement du fichier est *C:\RECYCLER* pour tous les fichiers supprimés. Cliquez sur le titre *Emplacement* pour afficher tous les fichiers rangés sous un emplacement de fichier ou de dossier particulier.

**Dernier modifié:** Cette colonne affiche la dernière date à laquelle le fichier a été modifié avant d'être supprimé. Cela peut être utile pour identifier un fichier que vous souhaiteriez récupérer. Cliquez le titre *Dernier modifié* pour lister les résultats du plus ancien au plus récent.

**Taille:** Cette colonne affiche la taille des fichiers. Cliquez sur *Taille* pour lister les fichiers du plus grand au plus petit, ou du plus petit au plus grand.

**État:** Cette colonne indique dans quelle mesure il est possible de récupérer un fichier et correspond à l'icône de l'état du fichier dont il est question à la Figure 6 ci-dessous. Cliquez sur *Etat* pour trier les fichiers par catégorie, de *Excellent* à *Irrécupérable*.

**Commentaire:** Cette colonne affiche les raisons pour lesquelles un fichier peut ou non être récupéré, et indique si un fichier supprimé a été ou non écrasé dans la *Table de fichiers maîtres (MFT)*. Cliquez sur *Commentaire* pour voir dans quelle mesure un fichier ou un groupe de fichiers a été écrasé.

Chaque fichier est doté d'un icône de couleur qui indique dans quelle mesure chaque fichier peut être récupéré:

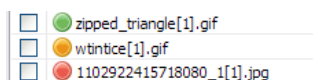


Figure 6: Les icônes d'état des fichiers

La liste suivante décrit chaque icône d'état:

- **Vert:** Excellente possibilité de récupérer le fichier au complet.
- **Orange:** Possibilité acceptable de récupérer le fichier.
- **Rouge:** Très faible possibilité de récupérer le fichier.

### 3.2 Comment exécuter un scan sans utiliser l'assistant de Recuva

Pour accéder directement à l'interface principale de Recuva, c.-à-d. sans passer par l'**Assistant de Recuva**, suivez les étapes énumérées ci-dessous:



**Première étape.** Cliquez sur Recuva ou sélectionnez **Démarrer > Programmes > Recuva > Recuva** pour afficher la Figure 1.

**Deuxième étape.** Cochez l'option *Ne plus afficher cet assistant au démarrage*, puis cliquez sur **Annuler** pour afficher la fenêtre suivante:

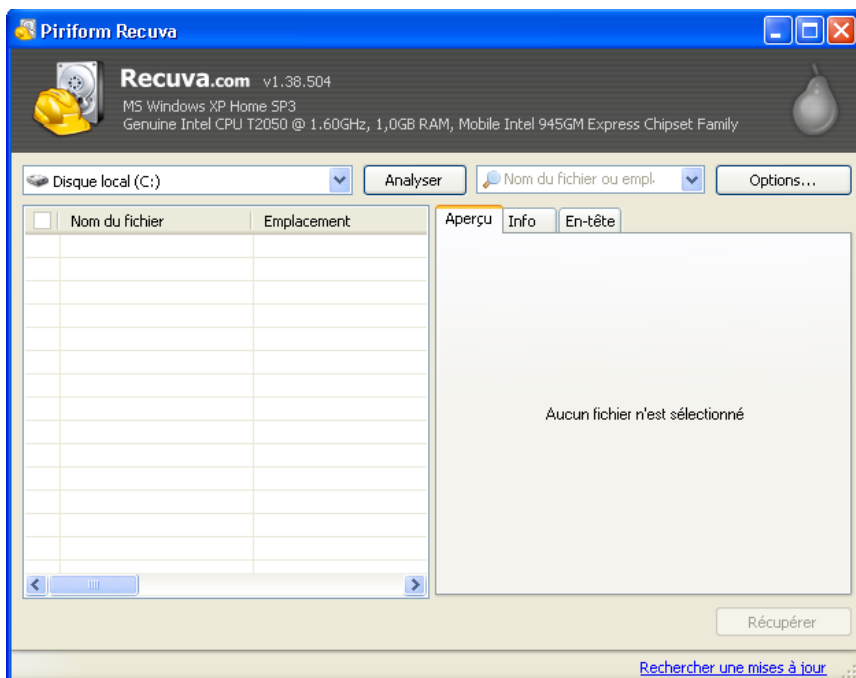


Figure 7: L'interface principale de Recuva

L'interface principale de *Piriform Recuva* est divisée en deux panneaux: le panneau des résultats, à gauche, et les onglets *Aperçu*, *Info* et *En-tête*, à droite, qui servent à trier et afficher les renseignements concernant un fichier supprimé en particulier. Vous pouvez y régler certaines options d'analyse similaires à celles qu'on retrouve dans l'assistant de *Recuva*.

**Troisième étape.** Cliquez sur le menu déroulant et **sélectionnez** le disque à analyser; le *Disque local (C:)* est sélectionné par défaut, et c'est celui qui est utilisé dans l'exemple suivant:

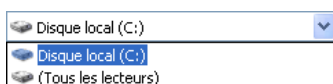


Figure 8: Le menu déroulant des disques à analyser

Le menu déroulant *Nom du fichier ou emplacement* vous permet de spécifier le type de fichier que vous recherchez, et correspond *grosso modo* aux catégories comprises dans la fenêtre *Type de fichiers de l'assistant de Recuva* illustrée à la Figure 2.

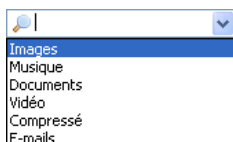


Figure 9: Le menu déroulant *Nom du fichier ou emplacement*

L'option *Nom du fichier ou emplacement* est une combinaison de zone de texte et de menu déroulant. Elle a deux fonctions principales: elle vous permet de chercher directement un fichier particulier, et/ou de trier un liste de fichiers supprimés par types de fichiers.

La même option l'option *Nom du fichier ou emplacement* peut être utilisée pour chercher des fichiers d'un type particulier ou de trier un liste générale de fichiers supprimés dans le panneau des résultats.


Pour retrouver un fichier dont le nom est connu (partiellement ou au complet), suivez les étapes énumérées ci-dessous:

**Première étape.** Saisissez le nom (ou la partie du nom que vous connaissez) du fichier que vous souhaitez récupérer comme suit (dans l'exemple suivant, nous cherchons le fichier *triangle.png*):



Figure 10: Le menu déroulant *Nom du fichier ou emplacement* affichant le nom de fichier *triangle.png*

**Astuce:** Cliquez sur  pour rafraîchir la zone de texte *Nom du fichier ou emplacement* (qui s'affiche estompée).

**Deuxième étape.** Cliquez sur  pour lancer la recherche du ou des fichier(s) supprimé(s); peu après, une fenêtre similaire à celle-ci s'affichera:

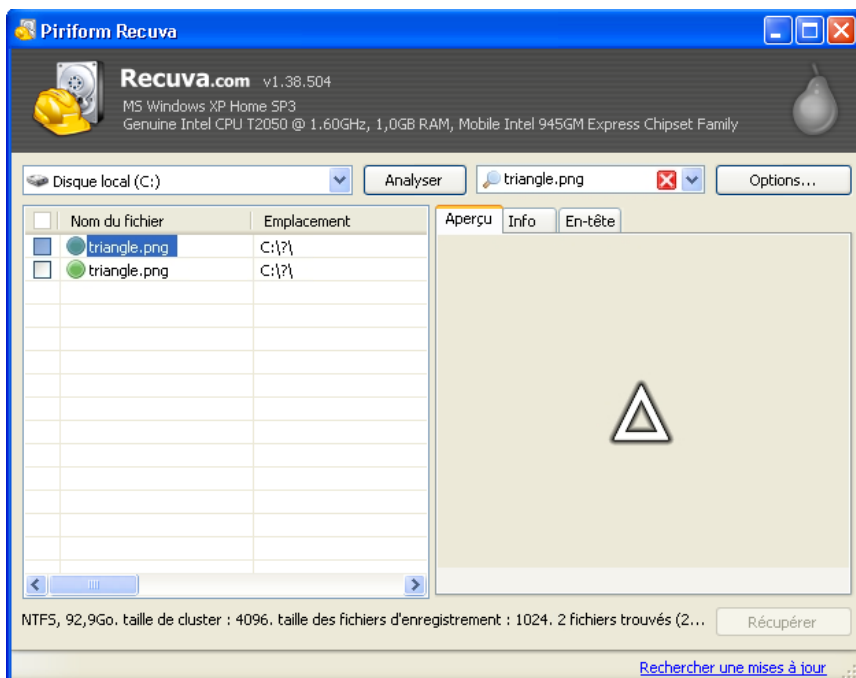


Figure 11: L'interface principale de Recuva affichant le fichier triangle.png dans l'onglet Aperçu

### 3.3 Comment exécuter une analyse approfondie avec Recuva

L'option *Analyse approfondie* vous permet d'exécuter un scan plus minutieux; bien entendu, une analyse approfondie prendra plus de temps, selon la vitesse de votre ordinateur et le nombre de fichiers à analyser. Cette option peut s'avérer utile si votre scan initial n'a pas trouvé les fichiers que vous souhaitez récupérer. Bien qu'une analyse approfondie puisse prendre plusieurs heures, selon la quantité de données stockées sur votre ordinateur, elle peut augmenter considérablement vos chances de récupérer les fichiers que vous cherchez.

L'option *Analyse approfondie* de **Recuva** peut également être activée en **cochant** l'option *Activer l'analyse approfondie* dans l'assistant de Recuva (veuillez vous référer à la Figure 4).

**Première étape.** Cliquez sur  pour afficher la fenêtre *Options*, puis **cliquez** sur l'onglet *Actions*:

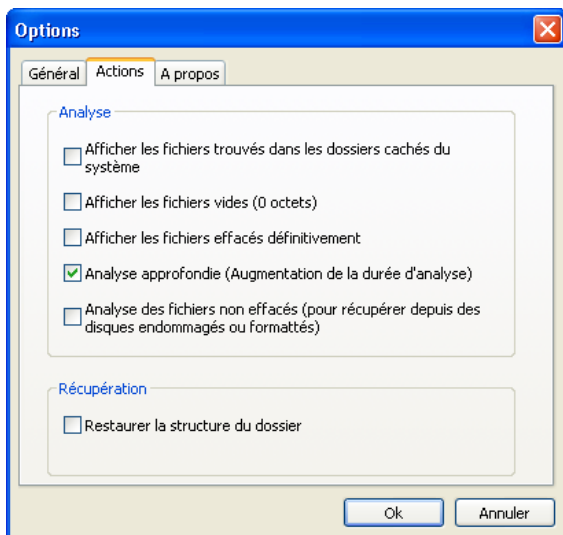


Figure 12: La fenêtre Options affichant l'onglet Actions

**Deuxième étape.** **Cochez** l'option *Analyse approfondie (augmentation de la durée d'analyse)*, puis **cliquez** sur .

**Troisième étape.** Cliquez sur  pour chercher des fichiers supprimés à l'aide de la fonction *Analyse approfondie*. Il est possible que le scan prenne plusieurs heures, selon la taille du disque dur et la vitesse de l'ordinateur:

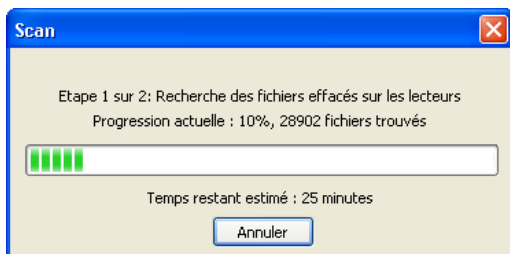
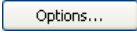


Figure 13: La fenêtre de progression du scan affichant le temps restant estimé pour compléter l'analyse approfondie

### 3.4 Une introduction à la fenêtre Options

Dans cette section, nous verrons comment utiliser les différents paramètres de la fenêtre *Options* pour récupérer et/ou écraser efficacement vos données privées ou sensibles. Pour régler ces paramètres, suivez les étapes énumérées ci-dessous:

**Première étape:** Cliquez sur  pour afficher la fenêtre suivante:

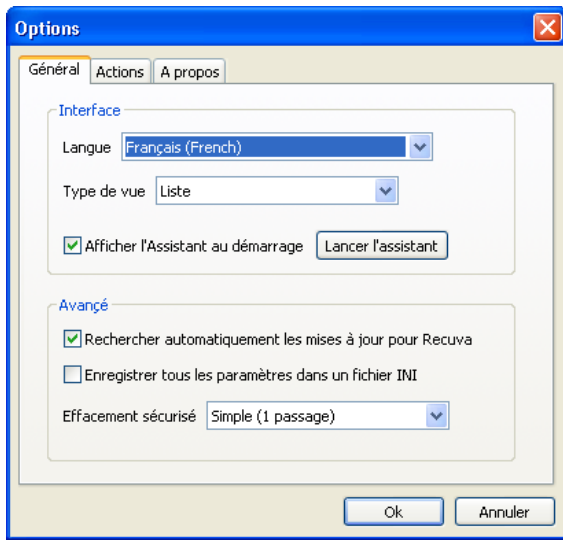


Figure 14: La fenêtre Options affichant l'onglet Général par défaut

La fenêtre *Options* est divisée en trois onglets: *Général*, *Actions* et *À propos*.

L'onglet *Général* vous permet de définir un ensemble de paramètres importants, dont la *Langue* (Recuva supporte 37 langues), le *Type de vue* et la possibilité d'activer ou de désactiver l'*Assistant de Recuva*.

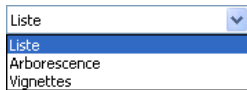


Figure 15: Le menu déroulant de l'option Type de vue

L'option **Type de vue** vous permet de choisir la façon dont s'afficheront les fichiers supprimés. Cette option peut aussi être activée en **\*\*cliquant à droite\*** sur un fichier dans l'interface *Piriform Recuva*.

- **Liste:** Cette option vous permet d'afficher les fichiers supprimés sous forme de liste, tel qu'illustré à la *Figure 5*.
- **Arborescence:** Cette option vous permet d'afficher l'emplacement des fichiers supprimés sous forme d'arborescence extensible.
- **Vignettes:** Cette option vous permet d'afficher les fichiers supprimés sous forme de graphiques ou d'images lorsque cela est possible.

La section *Avancé* de l'onglet *Général* vous permet de déterminer le nombre de fois que vos données seront écrasées par des données aléatoires pour empêcher que des parties malveillantes soient en mesure de les récupérer.

Le menu déroulant *Effacement sécurisé* affiche quatre options distinctes pour écraser vos données privées. Le mode par défaut est *Simple (1 passage)*, tel qu'illustré à la *Figure 14*. Les *passages* sont les fois que vos documents, fichiers ou dossiers seront écrasés avec des données aléatoires pour les rendre illisibles et irrécupérables.

**Deuxième étape:** Sélectionnez l'option *DOD 5220.22-M (3 passages)*:

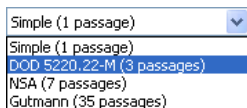


Figure 16: Le menu déroulant Effacement sécurisé avec l'option DOD 5220.22-M (3 passages) sélectionnée

Un passage simple peut être efficace pour écraser un document, un fichier ou un dossier donné; certaines personnes disposent des ressources et des capacités nécessaires pour récupérer des données relativement peu écrasées. L'option de trois passages constitue un équilibre entre la durée exigée pour écraser des données de façon sécurisée, d'une part, et la capacité de récupérer ces documents, fichiers ou dossiers, d'autre part.

**Troisième étape.** Cliquez sur  pour sauvegarder vos paramètres de l'onglet *Général*.

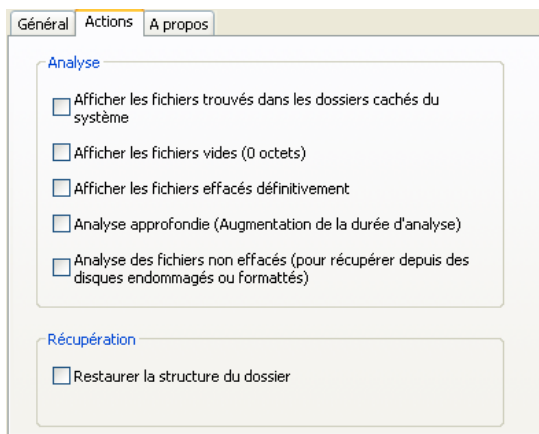


Figure 17: La fenêtre Options affichant l'onglet Actions

- **Afficher les fichiers trouvés dans les dossiers cachés du système:** Cette option vous permet d'afficher des fichiers qui se trouvent dans des répertoires cachés du système.
- **Afficher les fichiers vides (0 octets):** Cette option vous permet d'afficher des fichiers qui ne comportent pas ou très peu de contenu, et qui sont pratiquement irrécupérables.
- **Afficher les fichiers effacés définitivement:** Cette option vous permet d'afficher dans le panneau des résultats des fichiers qui ont été effacés de façon sécurisée.

**Commentaire:** Si vous avez déjà utilisé **CCleaner** ou un programme similaire, ce dernier change le nom du fichier pour **ZZZZZZ.ZZZ** lorsqu'il efface un fichier de façon sécurisée.

- **Analyse approfondie:** Cette option vous permet de scanner un disque dur au complet pour retrouver un document ou un fichier supprimé; si les analyses précédentes n'ont pas suffit à retrouver le fichier, l'*analyse approfondie* pourrait s'avérer utile. Par contre, il faut être conscient que cette méthode prend beaucoup plus de temps. Veuillez consulter la section **3.3 Comment exécuter une analyse approfondie avec Recuva**.
- **Analyse des fichiers non effacés (pour récupérer depuis des disques endommagés ou formatés):** Cette option vous permet d'essayer de récupérer des fichiers sur des disques qui ont subi des dommages physiques ou une corruption due à l'action de logiciels.

L'onglet *À propos* affiche des renseignements sur la version du programme, ainsi que des liens vers le site Internet de Piriform.

Maintenant que vous avez acquis la confiance nécessaire pour exécuter différents types de scans et que vous vous êtes familiarisé avec les paramètres des onglets *Général* et *Actions* de la fenêtre *Options*, nous pouvons voir comment récupérer ou effacer vos données privées ou sensibles à la section **4.0 Comment récupérer et/ou effacer des fichiers avec Recuva** <sup>[110]</sup>

## Comment récupérer et/ou effacer des fichiers avec Recuva

Sommaire des sections de cette page:

- **[4.0 Avant de commencer](#)**
- **[4.1 Comment récupérer un fichier supprimé](#)**
- **[4.2 Comment utiliser le menu contextuel](#)**
- **[4.3 Comment effacer un fichier supprimé](#)**

### 4.0 Avant de commencer

Dans cette section, nous verrons comment récupérer des fichiers préalablement supprimés et comment effacer (ou écraser) des données privées ou sensibles.

**Recuva** vous permet de créer un nouveau dossier pour y sauvegarder vos fichiers et documents récupérés. Même si **Recuva** vous laisse choisir un dossier pré-existant, pour des raisons de sécurité, il est recommandé de sauvegarder vos fichiers récupérés sur un support amovible, comme un disque dur externe ou une clé USB.

**Important:** Bien que **Recuva** soit très efficace pour écraser des données, il est possible que le programme laisse derrière lui des identifiants de fichiers qui peuvent révéler l'existence de ces fichiers. Pour protéger votre sécurité et votre confidentialité, il est plus logique de sauvegarder toutes vos données importantes, privées ou sensibles sur des dispositifs amovibles plutôt qu'à l'emplacement original des fichiers.

### 4.1 Comment récupérer un fichier supprimé

Pour récupérer un fichier supprimé, suivez les étapes énumérées ci-dessous:

**Première étape. Connectez** un disque dur externe ou une clé USB à votre ordinateur.

**Deuxième étape. Cochez** la case à cocher qui correspond au fichier que vous souhaitez récupérer pour activer le bouton *Récupérer...* ou **double cliquez** ce fichier pour cocher et surligner ce fichier simultanément.

**Troisième étape.** Cliquez sur  pour afficher la fenêtre *Rechercher un dossier*.

**Quatrième étape.** Sélectionnez une destination puis cliquez sur  afin de créer un dossier pour vos fichiers récupérés, tel qu'illustré à la *Figure 1* ci-dessous.

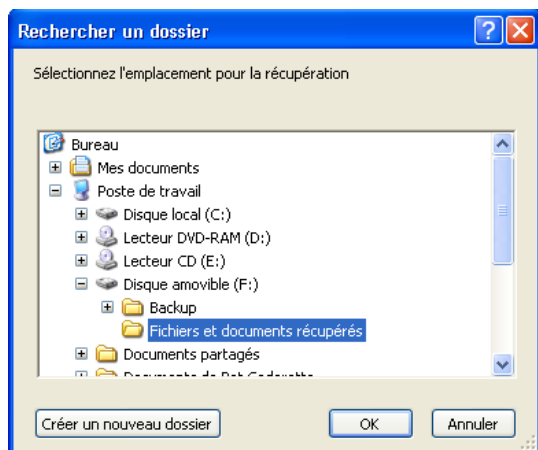


Figure 1: La fenêtre *Rechercher un dossier* affichant le nouveau dossier créé sur un disque du dur externe

**Commentaire:** Dans cet exemple, le nouveau dossier s'est vu donner un nom explicite. Cependant, toujours dans l'optique de préserver votre confidentialité et votre sécurité numérique, nous vous encourageons à donner un nom plus discret au dossier que vous créez pour y sauvegarder vos données privées et sensibles.

**Cinquième étape.** Cliquez sur  pour lancer le processus de récupération de vos fichiers supprimés; vous verrez apparaître une fenêtre affichant une barre de progression, tel qu'illustré ci-dessous:

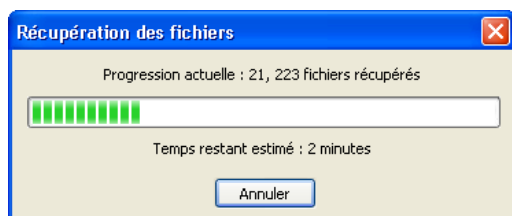


Figure 2: La barre de progression du processus de récupération des fichiers

Lorsque les fichiers seront récupérés, une fenêtre de confirmation s'affichera:

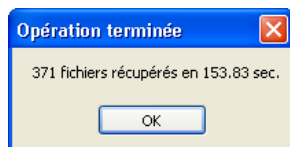


Figure 3: La fenêtre *Opération terminée*

**Commentaire:** **Recuva** peut récupérer plusieurs fichiers en une seule opération. Vous n'avez qu'à cocher tous les fichiers que vous souhaitez récupérer et suivre les consignes des **étapes 4 à 5**.

Maintenant que vous savez comment récupérer des fichiers supprimés, nous verrons maintenant comment utiliser le menu contextuel pour exécuter une récupération de plusieurs fichiers et/ou écraser des fichiers.

## 4.2 Comment utiliser le menu contextuel

**Recuva** offre différentes options pour sélectionner des documents, fichiers ou dossiers que vous souhaiteriez récupérer ou écraser.

- **Cocher:** Habituellement, on coche pour sélectionner rapidement plusieurs fichiers non contigus ou séparés afin de les récupérer ou les écraser.
- **Surligner:** Habituellement, on surligne pour sélectionner rapidement plusieurs fichiers contigus en bloc ou en groupe afin de les récupérer ou les écraser.

**Cliquez à droite** sur un fichier supprimé affiché dans l'interface principale de **Recuva** pour afficher le menu contextuel suivant:

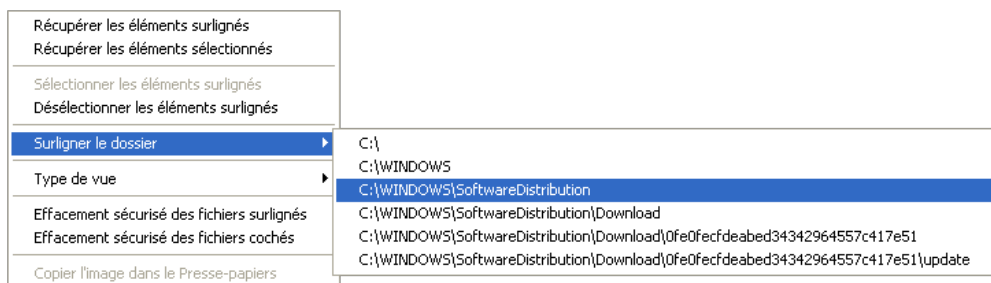


Figure 4: Le menu contextuel

**Récupérer les éléments surlignés:** Cette option vous permet de récupérer tous les fichiers que vous avez surlignés.

**Récupérer les éléments sélectionnés:** Cette option vous permet de récupérer un fichier dont vous avez coché la case à cocher.

**Sélectionner les éléments surlignés:** Cette option vous permet de cocher le(s) fichier(s) surligné(s).

**Dessélectionnez les éléments surlignés:** Cette option vous permet de décocher les fichiers surlignés.

Comme nous l'avons vu, le **Type de vue** peut également être défini dans l'onglet *Général* de la fenêtre *Options*. Cette option-ci vous permet de définir les fichiers supprimés s'afficheront.

- **Liste:** Cette option vous permet d'afficher les fichiers supprimés sous forme de liste, tel qu'illustré à la *Figure 5*.
- **Arborescence:** Cette option vous permet d'afficher l'emplacement des fichiers supprimés sous forme d'arborescence extensible.
- **Vignettes:** Cette option vous permet d'afficher les fichiers supprimés sous forme de graphiques ou d'images lorsque cela est possible.

**Surligner le dossier:** Cette option vous permet de sélectionner plusieurs fichiers supprimés en fonction de leur chemin d'accès au répertoire, et d'exécuter sur eux les actions listées dans le menu contextuel.

**Effacement sécurisé des fichiers surlignés:** Cette option vous permet d'effacer le fichier supprimé surligné.

**Effacement sécurisé des fichiers cochés:** Cette option vous permet d'effacer un fichier supprimé, ce qui change son icône d'état du vert au rouge.

### 4.3 Comment écraser un fichier supprimé

Pour écraser/effacer un fichier supprimé, suivez les étapes énumérées ci-dessous:

**Première étape. Cochez** le fichier que vous voulez écraser/effacer, puis **cliquez à droite** sur la case à cocher pour afficher le menu contextuel.

**Deuxième étape. Sélectionnez**  *Effacement sécurisé des fichiers cochés* pour afficher la boîte de dialogue de confirmation suivante:

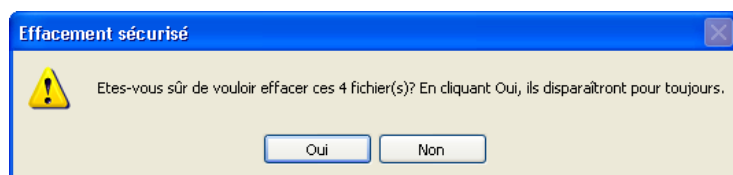


Figure 5: La boîte de dialogue de confirmation *Effacement sécurisé*

**Troisième étape. Cliquez** sur  pour lancer le processus d'effacement; selon la taille et l'état du fichier, ainsi que le paramètre de l'*Effacement sécurisé* que vous avez défini dans l'onglet *Général* de la fenêtre *Options*, cette opération peut prendre un certain temps. Lorsque le processus d'effacement est complété, une fenêtre comme celle-ci s'affiche:

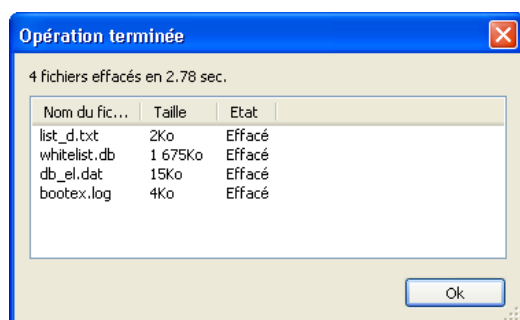


Figure 6: La fenêtre *Opération terminée*

Vous avez réussi à utiliser **Recuva** pour récupérer et effacer des fichiers préalablement supprimés. Pour réviser votre connaissance du programme **Recuva** veuillez consulter la section **FAQ et questions récapitulatives** <sup>[111]</sup>

## Faq et questions récapitulatives

Elena et Nikolai sont enchantés par les possibilités que leur offre **Recuva**, et surtout par la facilité d'utilisation et l'efficacité du programme. Ils sont maintenant curieux de connaître ses options avancées et ont quelques questions supplémentaires.

**Q:** Y a-t-il des types de fichiers que **Recuva** ne peut pas récupérer?

**A:** Non, **Recuva** peut récupérer n'importe quel type de fichiers.

**Q:** Est-ce que je peux récupérer un fichier qui a été écrasé/effacé de façon sécurisée?

**A:** Une fois qu'un fichier a été effacé de façon sécurisée, il est disparu pour toujours.

**Q:** J'ai remarqué que parfois, même après qu'un fichier ait été effacé, il reste identifié comme récupérable. Comment est-ce possible?

**A:** Il est possible que ce que tu vois est un identifiant de fichier, une balise indiquant l'emplacement original du fichier. Par contre, si tu récupères et que tu ouvres ce fichier, tu verras que son contenu est illisible.

**Q:** J'ai supprimé un fichier par accident; comme je l'avais créé à peine cinq minutes auparavant, je croyais qu'il allait être assez facile de le récupérer. Comment se fait-il que **Recuva** soit incapable de le récupérer?

**\*A:** Ironiquement, un document ou un fichier qui n'existe que depuis quelques minutes est plus susceptible d'être écrasé par des fichiers temporaires qu'un fichier qui existe depuis plus longtemps. **Recuva** ne récupère pas

facilement des fichiers qui ont été supprimés peu après leur création.\*

**Q:** Suite à un nettoyage de mon système à l'aide de **CCleaner**, est-ce que mes données pourraient être récupérées?

**\*A:** Selon les ressources et les aptitudes de la personne qui tenterait une telle récupération, c'est effectivement possible. Cela dépend aussi des paramètres de l'effacement sécurisé qui ont été définis pour nettoyer les fichiers

temporaires et le **Registre de Windows** avec **CCleaner**. Pour réduire au maximum la possibilité de récupérer des données privées ou sensibles, il est conseillé d'activer l'option Effacement sécurisé dans **CCleaner**, puis d'effacer

l'espace libre du disque dur et du **Windows Master File Table**. Dans **Recuva**, il est possible d'augmenter le nombre de passages utilisés pour écraser des données. C'est une bonne question parce qu'on peut voir comment différents outils peuvent être combinés pour protéger ta confidentialité et ta

sécurité numérique.\*

## 5.1 Questions récapitulatives

- Est-ce que le fait de fermer votre ordinateur réduit la capacité de **Recuva** à récupérer efficacement vos documents, fichiers et dossiers supprimés?
- En quoi le fait d'augmenter le nombre de passages à un effet sur l'effacement sécurisé d'un document ou d'un fichier donné?
- Nommez deux conditions qui ont un effet sur votre capacité à récupérer un document un fichier supprimé dans **recuva**.
- Il y a deux façons d'activer l'*Analyse approfondie* dans **recuva**; quelles sont-elles?
- Dans quelle circonstance est-il indiqué d'utiliser l'*Assistant de Recuva* pour lancer un scan et tenter de récupérer des fichiers supprimés?

## Eraser - suppression de fichiers sécurisée

**Eraser** permet de nettoyer votre ordinateur en supprimant définitivement les fichiers sensibles qui s'y trouvent. Il peut également être utilisé pour nettoyer des dispositifs de stockage amovibles.

### Site Internet

[www.heidi.ie](http://www.heidi.ie) <sup>[112]</sup>

### Configuration requise :

- Windows 95, 98, ME, NT 4.0, 2000, XP & Vista

### Version utilisée pour rédiger ce guide :

- 5.86

### Licence :

- FLOSS (Free/Libre and Open Source Software)

### Pour installer Eraser

- Lisez la courte introduction des *Guides pratiques* <sup>[89]</sup>
- **Cliquez sur l'icône ci-dessous et 'Ouvrez' ou 'Exécutez' l'assistant d'installation.** Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.

Eraser:



<sup>[113]</sup>

### Lecture préalable :

- Livret pratique Security in-a-box, chapitre 6. Détruire définitivement des données sensibles <sup>[114]</sup>.

**Niveau :** 1 : Débutant, 2 : **Moyen**, 3 : Intermédiaire, 4 : Expérimenté, 5: Avancé



Temps d'apprentissage : 20 minutes

Ce que vous apportera l'utilisation de cet outil :

- La capacité de supprimer définitivement de votre ordinateur des fichiers de nature « délicate ».
- La capacité de supprimer définitivement de votre ordinateur tous les fichiers récupérables qui sont actuellement invisibles.

### 1.1 À propos de cet outil

Eraser permet de nettoyer votre ordinateur en supprimant définitivement les fichiers sensibles qui s'y trouvent. Pour ce faire, il réécrit par dessus, ou « écrase », les données à effacer. Cette méthode permet de supprimer définitivement aussi bien des fichiers que des répertoires. De plus, Eraser effacera les copies de fichiers qui se trouvent sur votre ordinateur et dont vous ne soupçonnez peut-être même pas l'existence. Cela comprend les fichiers que vous avez déjà supprimés par l'interface de **Windows**, ainsi que les copies des documents sur lesquels vous avez travaillé dans le passé.

1. Eraser permet d'effacer les fichiers ponctuellement ou à intervalle régulier.
2. Si vous choisissez de le faire à intervalle régulier, il faut absolument que l'ordinateur soit allumé au moment prévu, sinon la suppression des fichiers ne sera pas effectuée.
3. Une fois qu'un fichier est supprimé par Eraser, il est impossible de le récupérer à l'aide d'un outil de récupération de données.
4. Pour plus de sécurité, il est recommandé d'écraser les fichiers entre trois et sept fois.
5. Eraser permet également de supprimer/réécrire tout l'espace libre restant sur votre ordinateur. Cela signifie qu'il peut supprimer toutes les traces de vos travaux passés (potentiellement récupérables parce qu'ils n'ont pas été supprimés définitivement).

Offline Installation Instructions :

Pour installer Eraser

- \*Lisez la courte **Introduction** aux **Guides pratiques** <sup>[1]\*\*</sup>
- **Cliquez sur l'icône Eraser ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.

Eraser:



[115]

## Comment régler les options d'Eraser

Tel que décrit au chapitre 6. **Détruire définitivement des données sensibles** <sup>[114]</sup> du livret pratique, **Eraser** supprime les données sur le disque en les écrasant avec d'autres données aléatoires. Plus le nombre de réécritures est élevé (pour écraser les fichiers), plus il sera difficile de les récupérer.

**Commentaire** : Nous recommandons d'écraser les données au moins trois fois.

**Conseil** : Notez que chaque « passe » de réécriture prend un certain temps et que plus le nombre de passes est élevé, plus long sera le processus de suppression du fichier. Évidemment, cet effet sera davantage ressenti lors de la suppression de fichiers volumineux ou lors de la suppression/réécriture de l'espace libre.

Le nombre de passes peut être choisi en accédant au menu *Preferences: Erasing*.

**Première étape. Sélectionnez: Edit > Preferences > Erasing**, comme suit :

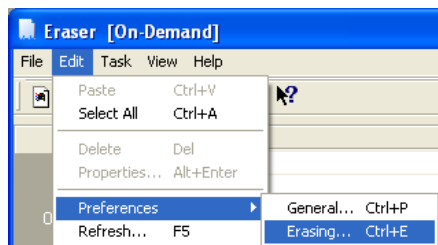


Figure 1 : La fenêtre Eraser [On-demand] affichant les options du menu Edit

La fenêtre Preferences:Erasing s'affiche comme suit :

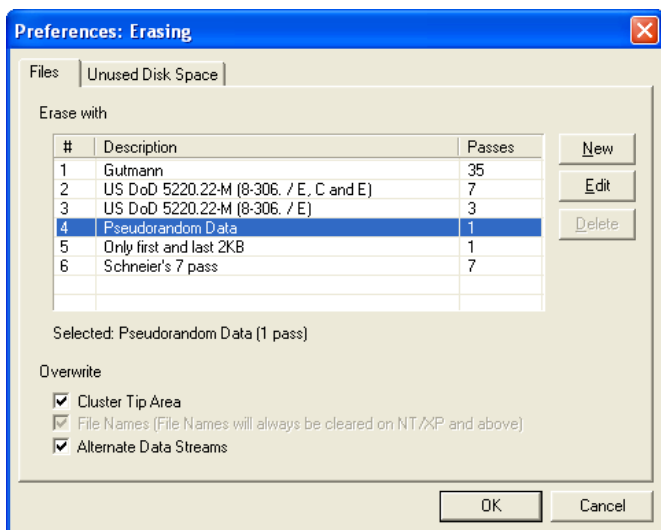


Figure 2 : La fenêtre Preferences: Erasing

La fenêtre Preferences: Erasing décrit la méthode utilisée pour la suppression/réécriture des fichiers.

Description: Les noms des procédures de réécriture sont affichés dans cette colonne.

Passes: Le nombre de passes de réécritures utilisées pour chaque méthode.

Nous allons écraser nos données en utilisant la méthode *Pseudorandom Data*. Par défaut, cette méthode comprend une seule passe de réécriture. Par souci de sécurité, nous allons augmenter cette valeur à 3.

**Deuxième étape. Sélectionnez :** # 4 *Pseudorandom Data*, tel qu'illustré à la figure 2.

**Troisième étape. Cliquez sur Edit** pour faire apparaître la fenêtre Passes, illustrée ci-dessous :

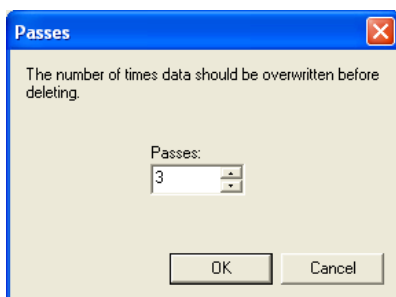


Figure 3 : La fenêtre Passes d'Eraser

**Quatrième étape.** Choisissez un nombre de passes entre 3 et 7 (prenez compte autant du temps requis pour chaque passe que du niveau de sécurité souhaité).

**Cinquième étape. Cliquez** sur le bouton OK pour revenir à la fenêtre Eraser Preferences: Erasing.

L'option # 4 Pseudorandom Data devrait maintenant ressembler à ceci :

#	Description	Passes
1	Gutmann	35
2	US DoD 5220.22-M (8-306. / E, C and E)	7
3	US DoD 5220.22-M (8-306. / E)	3
4	Pseudorandom Data	3

Figure 4 : La fenêtre Preferences: Erasing avec l'option 4 sélectionnée.

**Conseil :** Assurez-vous que les options *Cluster Tip Area* et *Alternate Data Streams* sont sélectionnées (elles devraient l'être par défaut).

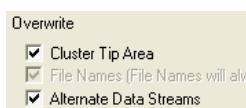


Figure 5 : Les options Cluster Tip Area et Alternate Data Streams sélectionnées par défaut.

- *Cluster Tip Area* : Un disque dur est divisé en plusieurs segments que l'on nomme *clusters* ou « blocs ». Habituellement, un fichier est contenu sur plusieurs blocs, sans toutefois remplir complètement le dernier bloc qu'il occupe. La partie vacante à la fin du dernier bloc se nomme la *Cluster Tip Area* ou « Zone de fin de bloc ». Cette Zone de fin de bloc peut contenir une partie des données sensibles d'un autre fichier ayant précédemment occupé cet espace du bloc. Les données qui se trouvent dans cette zone peuvent être récupérées par un spécialiste. Assurez-vous donc de **cocher** cette case!
- *Alternate Data Streams* : Un fichier stocké sur un ordinateur peut comporter plusieurs parties. Par exemple, le présent document contient du texte et des images. Ces différents éléments sont stockés à différents emplacements du disque : c'est ce que sont les *streams* ou « trames de données ». **Cocher** cette option vous assure que toutes les

« Trames de données alternatives » associées aux fichiers seront effacées.

**Sixième étape. Cliquez** sur le bouton *OK*.

Vous venez de configurer la méthode utilisée pour écraser les fichiers dans Eraser. Vous devriez choisir les mêmes options dans l'onglet suivant de la fenêtre *Preferences* : *Erasing*, c.-à-d. l'onglet *Unused Disk Space*. Cela dit, tenant en considération que chaque passe prendra environ deux heures, vous pouvez y spécifier un nombre de passes moins élevé.

## Comment utiliser Eraser

### 3.1 Comment utiliser Eraser avec Windows Explorer

L'application la plus fréquente d'**Eraser** ne passe pas par le programme lui-même, mais plutôt par la fenêtre du *Poste de travail* de l'**Explorateur Windows**.

**Première étape. Ouvrez** un dossier où se trouve un fichier que vous souhaitez supprimer définitivement.

**Deuxième étape. Cliquez à droite** sur le fichier voulu. Deux nouvelles options s'offrent maintenant à vous dans le menu défilant, c.-à-d. *Erase* et *Eraser Secure Move*.

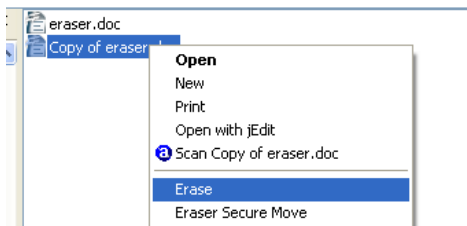


Figure 6. Les options *Erase* et *Eraser Secure Move*

Nous utiliserons l'option *Erase* pour supprimer ce fichier définitivement.

**Troisième étape. Sélectionnez** : *Erase* dans le menu.

Vous verrez alors apparaître la boîte de dialogue *Confirm Erasing*, illustrée ci-dessous :

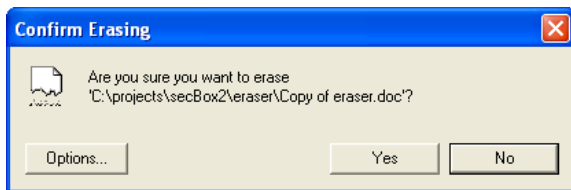


Figure 7 : La boîte de dialogue *Confirm Erasing*

Si le fichier décrit correspond bien à celui que vous souhaitez supprimer définitivement, passez à l'étape suivante :

**Quatrième étape. Cliquez** sur le bouton *Yes*.

Le fichier sera alors supprimé définitivement du système.

**Avertissement** : Lorsque vous effacez un fichier de cette façon, il est perdu à jamais. Vous ne pourrez PAS le récupérer. Assurez vous de n'effacer que les fichiers que vous ne voulez pas conserver sur votre ordinateur.

Pour transférer un ou plusieurs fichiers de façon sécurisée d'un emplacement à un autre (par exemple de votre ordinateur à une clé USB) :

**Cinquième étape. Sélectionnez** : *Eraser Secure Move*.

Vous devrez répondre au même message d'avertissement que précédemment pour continuer.

### 3.2 Comment « nettoyer » l'espace libre du disque dur

Le nettoyage, ou la réécriture, de l'espace inutilisé du disque dur implique la suppression définitive de toutes les traces des fichiers qui se trouvaient préalablement dans « l'espace libre » de votre disque dur ou de votre dispositif de stockage amovible. Cet espace vide peut contenir des fichiers qui n'ont pas été intégralement supprimés. (À ce sujet, voir le [guide pratique Undelete Plus](#) <sup>[116]</sup> et le [chapitre 6](#) <sup>[114]</sup> du livre pratique *Security in-a-box*.)

**Première étape. Sélectionnez** : *Démarrer > Programmes > Eraser > Eraser*

**Conseil** : Vous pouvez soit lancer une tâche ponctuelle de nettoyage de l'espace libre, soit planifier une tâche automatique à intervalle régulier.

**Important** : Ce processus peut prendre de 2 à 5 heures et ralentira votre ordinateur si vous l'utilisez en même temps. Il est donc conseillé de planifier une tâche de nettoyage de l'espace libre à un moment qui n'entre pas en conflit avec votre utilisation de l'ordinateur (par exemple, la nuit, quand vous ne travaillez pas).

### 3.3 Comment utiliser l'option de réécriture ponctuelle (*On-Demand*)

Pour créer une tâche de réécriture ponctuelle (*On-Demand*) pour effacer l'espace inutilisé du disque dur, suivez les étapes énumérées ci-dessous :



Première étape. Cliquez sur :

Deuxième étape. Sélectionnez : **File > New Task**, comme suit :

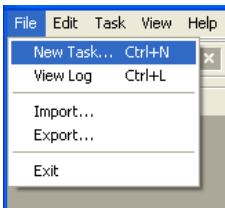


Figure 8 : Ouvrir une nouvelle tâche dans le menu File

L'option *Unused space on drive* devrait déjà être cochée.

Troisième étape. Sélectionnez le disque dont l'espace libre doit être nettoyé. (Dans l'exemple ci-dessous, le *disque local (C :)* est sélectionné. Il s'agit habituellement du disque principal sur la plupart des ordinateurs.)

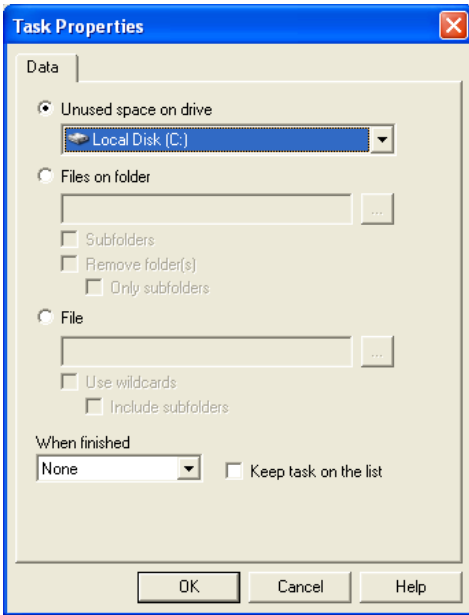


Figure 9 : La fenêtre Task Properties d'Eraser

Quatrième étape. Cliquez sur le bouton **OK**.

La tâche est maintenant créée et devrait être lancée automatiquement. La nouvelle tâche devrait être affichée dans la fenêtre principale d'Eraser.

Cinquième étape. Cliquez à droite sur la tâche pour activer le menu défilant illustré ci-dessous :

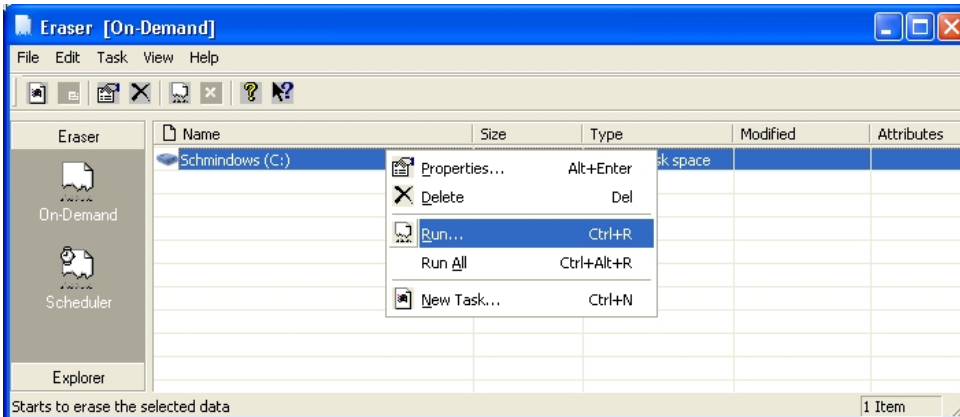


Figure 10 : La fenêtre principale d'Eraser avec l'option Run sélectionnée

Sixième étape. Sélectionnez : **Run** pour activer la boîte de dialogue suivante :

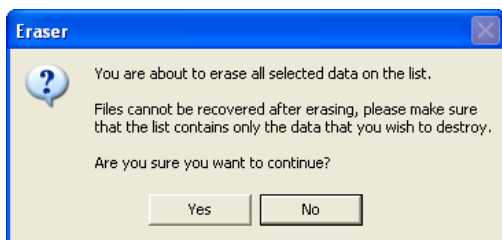


Figure 11. La boîte de dialogue Eraser

**Septième étape.** Cliquez sur le bouton Yes.

Une barre de progrès apparaît, et Eraser procède au nettoyage de l'espace vide.

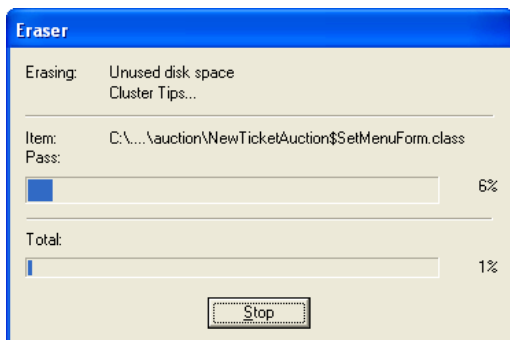


Figure 12 : La fenêtre d'Eraser

### 3.4 Comment utiliser l'option de nettoyage par tâche planifiée

Comme il est souvent trop facile d'oublier d'entretenir son ordinateur convenablement, **Eraser** offre la possibilité de lancer automatiquement les tâches de nettoyage à intervalle quotidien ou hebdomadaire, à une heure définie d'avance.



**Première étape.** Cliquez sur : Scheduler dans la fenêtre principale d'Eraser.

**Deuxième étape.** Sélectionnez : **File > New Task**, comme suit :

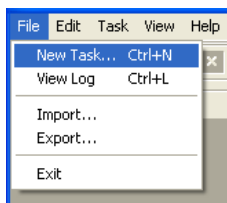


Figure 13 : Ouvrir une nouvelle tâche dans le menu File

La fenêtre qui s'affiche alors ressemble à celle qui nous a permis de définir une tâche ponctuelle.

**Troisième étape.** Réglez ces options comme précédemment, à la section **3.3 Comment utiliser l'option de suppression/récriture ponctuelle**.

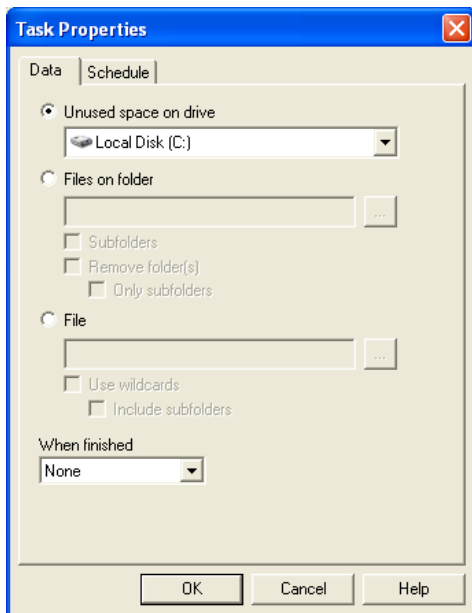


Figure 14 : La fenêtre Task Properties d'Eraser affichant l'onglet Schedule

**Quatrième étape.** Cliquez sur l'onglet *Schedule*.

L'onglet *Schedule* affiche les options suivantes :

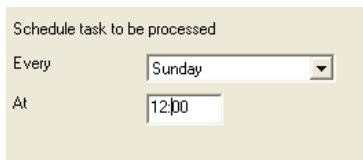


Figure 15 : L'onglet Schedule d'Eraser

**Commentaire :** En cliquant sur le menu déroulant *Every*, vous aurez le choix de lancer la tâche à intervalle quotidien ou hebdomadaire. La deuxième option permet de choisir l'heure à laquelle vous souhaitez lancer la tâche.

**Cinquième étape.** Après avoir défini l'intervalle de la tâche, **cliquez** sur le bouton **OK**.

La tâche planifiée s'affichera comme ceci :

Local Disk (C:)	Unused disk space	26/08/2007 1...	Every Sunday
-----------------	-------------------	-----------------	--------------

Figure 16 : La liste des tâches planifiées d'Eraser

**Commentaire :** Pour que la tâche planifiée soit exécutée, il est nécessaire que l'ordinateur soit en fonction à l'heure choisie pour la tâche.

### 3.5 Comment éliminer une tâche

Après avoir lancé ou planifié une tâche, vous voudrez peut-être l'enlever de votre liste de tâches.

Pour éliminer une tâche ponctuelle, suivez les étapes énumérées ci-dessous :



**Première étape.** Cliquez sur : **On-Demand** pour afficher la liste des tâches, tel qu'illustré ci-dessous :

Name	Size	Type	Modified	Attributes
C:\temp\		File Folder	20/06/2007 14:...	
Local Disk (C:)	43552 MB	Unused disk space		

Figure 17 : La liste des tâches d'Eraser

**Deuxième étape.** Sélectionnez la tâche que vous souhaitez éliminer (la tâche sélectionnée sera surlignée en bleu, tel qu'illustré dans la figure 17).

**Troisième étape.** Cliquez sur : **X**

La tâche sera alors retirée de la liste.

Name	Size	Type	Modified	Attributes
C:\temp\		File Folder	20/06/2007 14:...	

Figure 18 : La liste des tâches d'Eraser, avec la tâche ponctuelle en moins

La procédure pour éliminer une tâche planifiée est pratiquement identique. Pour ce faire, suivez les étapes énumérées ci-dessous :



Première étape. Cliquez sur :

Répétez les étapes 2 et 3 énumérées ci-dessus pour éliminer une tâche ponctuelle.

## Faq et questions récapitulatives

Elena et Nikolai trouvent **Eraser** assez facile à utiliser, mais ils se rendent bien compte que c'est un programme qui doit être manipulé avec précaution, puisque les éléments qui sont supprimés de cette façon seront irrécupérables. Ils ont l'impression qu'il est important de prendre le temps d'apprendre à bien connaître le programme avant de s'en servir régulièrement. Eraser semble bien fonctionner sur l'ordinateur d'Elena, mais ils ont encore quelques questions à propos d'Eraser.

**Q.** : Puis-je utiliser Eraser pour supprimer des fichiers qui se trouvent sur ma clé USB?

**R.** : Oui. Tu peux supprimer ces fichiers définitivement par l'interface **Explorateur Windows**. Tu peux également effacer/réécrire l'espace libre sur ta clé USB en créant une tâche appropriée dans Eraser.

**Q.** : Si je ne veux plus utiliser Eraser, est-ce qu'il est facile de désinstaller le programme? Et si je le désinstalle, est-ce que cela aura un effet sur mon ordinateur? Et mes fichiers demeureront-ils supprimés?

**R.** : Tu peux désinstaller Eraser à partir du menu Démarrer. Sélectionne **Démarrer > Programmes > Eraser > Uninstall Eraser**. Cela n'affectera en rien les autres programmes installés sur ton ordinateur, et les fichiers que tu as déjà supprimés ne seront pas récupérables.

**Q.** : Y a-t-il des fichiers **Windows** qu'Eraser ne supprime pas?

**R.** : Tous les fichiers qui se trouvent sur ton ordinateur peuvent être supprimés définitivement par Eraser. Même certains fichiers invisibles (tel que les fichiers récupérables se trouvant dans l'espace libre) seront supprimés définitivement si tu configures adéquatement les options que nous avons vues.

**Q.** : Est-ce qu'Eraser supprime aussi les noms des fichiers?

**R.** : Oui, toutes les parties du fichier sont supprimées définitivement. Cependant, tu devrais utiliser **CCleaner** <sup>[117]</sup> pour supprimer la liste des documents récents.

**Q.** : Est-ce qu'il sera possible à quelqu'un d'accéder aux fichiers supprimés?

**R.** : La récupération des données de fichiers qui ont été écrasés est un processus extrêmement complexe et onéreux. Le temps requis pour restaurer un fichier qui n'a été écrasé qu'une seule fois est démesuré, alors imagine le temps qu'il faut pour restaurer un fichier écrasé de trois à sept fois! Si tu utilises Eraser de façon adéquate, tu peux être certain que tes données ont été supprimées définitivement.

### 4.1 Questions récapitulatives

1. Quel genre d'information Eraser peut-il effacer de votre ordinateur?
2. Qu'entend-on par « espace libre / inutilisé »?
3. Comment Eraser supprime-t-il vos données?
4. Quel est le nombre de passes minimum recommandé avec Eraser?
5. Comment configure-t-on le nombre de passes minimum dans Eraser?
6. Comment planifie-t-on une tâche automatique dans Eraser?
7. Comment peut-on effacer un répertoire qui se trouve dans un autre répertoire?
8. Comment peut-on effacer plusieurs fichiers à la fois?

## CCleaner - suppression de fichiers et nettoyage sécurisés

### Short Description:

**CCleaner** est un programme efficace et facile à utiliser pour protéger votre sécurité et votre confidentialité numérique. En supprimant de façon permanente votre historique de navigation, vos cookies et autres fichiers temporaires générés automatiquement lors de vos séances de travail, et en nettoyant l'espace libre de vos disques durs, **CCleaner** limite les moyens par lesquels des tiers hostiles ou malveillants pourraient contrôler vos préférences et habitudes de travail ou infecter votre système.

### Online Installation Instructions:

#### Pour installer CCleaner

- Lisez la courte **Introduction aux Guides pratiques** <sup>[1]</sup>
- Cliquez sur l'icône **CCleaner** ci-dessous pour ouvrir la page de téléchargement [www.piriform.com/ccleaner/builds](http://www.piriform.com/ccleaner/builds)
- Dans la section 'CCleaner - Slim' cliquez sur le bouton de 'téléchargement'
- **Sauvegardez** l'exécutable 'ccsetup\_slim.exe' sur votre ordinateur, puis **double-cliquez** sur l'icône pour lancer l'installation du programme
- Lisez attentivement les 'consignes d'installation' détaillées à la prochaine section avant de continuer

- Après avoir complété l'installation de **CCleaner** vous pouvez supprimer l'exécutable d'installation de votre ordinateur

CCleaner:



Site Internet

[www.ccleaner.com](http://www.ccleaner.com) [119]

Configuration requise

- Compatible avec toutes les versions de Windows

Version utilisée pour rédiger ce guide

- 4.03

Licence

- Gratuitiel

Lecture préalable

Livret pratique Security-in-a-Box, chapitre [6. Détruire définitivement des données sensibles](#) [37]

Niveau: 1: Débutant, 2: Moyen, 3: Intermédiaire, 4: Expérimenté, 5: Avancé

Temps d'apprentissage: 15 minutes

Ce que vous apportera l'utilisation de cet outil:

- La capacité de supprimer définitivement toutes traces de vos activités et des fichiers temporaires stockés sur votre ordinateur.
- La capacité de **nettoyer l'espace libre des disques** connectés à votre ordinateur
- La capacité de nettoyer le **Registre de Windows**
- La capacité de **déterminer quels programmes sont activés au démarrage de votre ordinateur**

Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

**BleachBit** [120] est un autre excellent outil de suppression et de destruction de fichiers temporaires, compatible avec **GNU Linux** et **Microsoft Windows**. **BleachBit** vous permet de supprimer les fichiers temporaires générés par 70 des applications les plus répandues et par le système d'exploitation, et de libérer de l'espace sur vos disques durs. Un programme de code source libre proposant une version portable, **BleachBit** est disponible en 32 langues. Les utilisateurs de **Ubuntu Linux** peuvent en outre se référer au guide [Nettoyer Ubuntu...](#) [121] pour apprendre à nettoyer leur système.

Les utilisateurs de **Mac OS** apprécieront sûrement les outils gratuits proposés par **Titanium's Software: OnyX et Maintenance** [122] pour supprimer les traces de vos séances de travail. Pour effacer de façon sécuritaire le contenu de votre *Trash*, ouvrez l'application *Finder* et sélectionnez le menu *Finder > Secure Empty Trash*. Vous pouvez choisir de toujours supprimer le contenu de votre *Trash* de façon sécuritaire en ouvrant les préférences *Avancées* du *Finder* et en cochant l'option *Empty Trash securely*. Pour nettoyer l'espace libre de votre disque dur, lancez l'application système *Disk Utility*, sélectionnez la partition voulue, sélectionnez l'onglet *Erase* et cliquez sur le bouton *Erase Free Space*.

## 1.1 À propos de cet outil

Les paramètres par défaut de votre système et de votre navigateur Web génèrent automatiquement une trace de vos données dont un tiers parti hostile ou malveillant pourrait tirer avantage, un peu comme un chasseur traquant sa proie. Chaque fois que vous utilisez un navigateur ou un logiciel de traitement de texte, ou tout autre programme, des fichiers et données temporaires sont générés et stockés quelque part sur votre ordinateur. Ces programme génèrent également des listes de documents ou pages Internet récemment consultés. Par exemple, chaque fois que vous saisissez une adresse Internet dans votre navigateur préféré, une liste des adresses qui commencent avec les mêmes caractères s'affichent automatiquement, comme ceci:

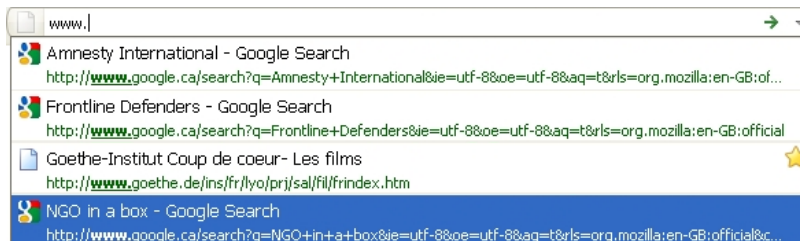


Figure 1: Une barre d'adresse de navigateur affichant différentes URLs

Bien que les historiques des navigateurs puissent être utiles à l'occasion, elle peuvent aussi permettre à un tiers parti d'identifier les sites Internet que vous avez visités. De plus, vos activités récentes peuvent être exposées par les données temporaires sauvegardées à partir des images comprises dans ces sites Internet, y compris les messages de courrier électronique et les coordonnées saisies dans des formulaires.

Pour supprimer les données temporaires générées chaque fois que vous utilisez un programme, il vous faudrait ouvrir chaque répertoire de chaque programme, identifier et supprimer manuellement chaque fichier temporaire. **CCleaner** affiche une liste de programmes et vous laisse choisir le ou les programme(s) dont vous souhaitez supprimer les fichiers temporaires.



**Important:** Même si **CCleaner** ne supprime que les fichiers temporaires, et non pas les documents sauvegardés sur votre ordinateur, il est **fortement recommandé** que vous conserviez une sauvegarde mise à jour de vos documents (veuillez consulter le **Livret pratique** Security-in-a-Box, chapitre **5. Récupérer des données perdues** [101] pour plus de conseils sur la création de copies de sauvegarde).

Après avoir lancé **CCleaner**, il est possible que vous ayez perdu les historiques de votre navigateur et de vos documents récents, ainsi que vos mots de passe sauvegardés. C'est précisément la fonction de cet outil, c'est-à-dire de minimiser les différentes façons par lesquelles des tiers partis malveillants pourraient infecter ou espionner votre système.

#### Offline Installation Instructions :

##### Pour installer CCleaner

- \*Lisez la courte **Introduction** aux **Guides pratiques** [1]\*\*
- **Cliquez sur l'icône CCleaner ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- *Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.*
- *Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.*

CCleaner:



## Comment installer et configurer CCleaner


Sommaire des sections de cette page:

- [2.0 Comment installer CCleaner](#)
- [2.1 Avant de commencer à configurer CCleaner](#)
- [2.2 Comment configurer CCleaner](#)

---

### 2.0 Comment installer CCleaner

L'installation de **CCleaner** est relativement simple et rapide. Pour lancer l'installation de **CCleaner**, suivez les étapes énumérées ci-dessous:

**Première étape.** Double-cliquez sur  pour lancer le processus d'installation. Il est possible que s'ouvre une boîte de dialogue *Fichier ouvert - Avertissement de sécurité*. Si c'est le cas, cliquez sur  pour afficher la fenêtre suivante:

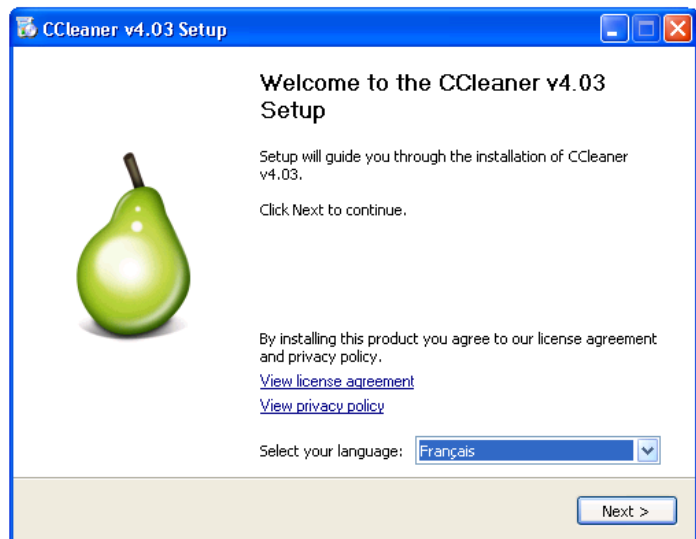


Figure 1: Bienvenue dans le programme d'installation de CCleaner v4.03

**Deuxième étape.** Cliquez sur  pour afficher la fenêtre *Options d'installation*, puis cliquez à nouveau sur  pour afficher la fenêtre suivante :

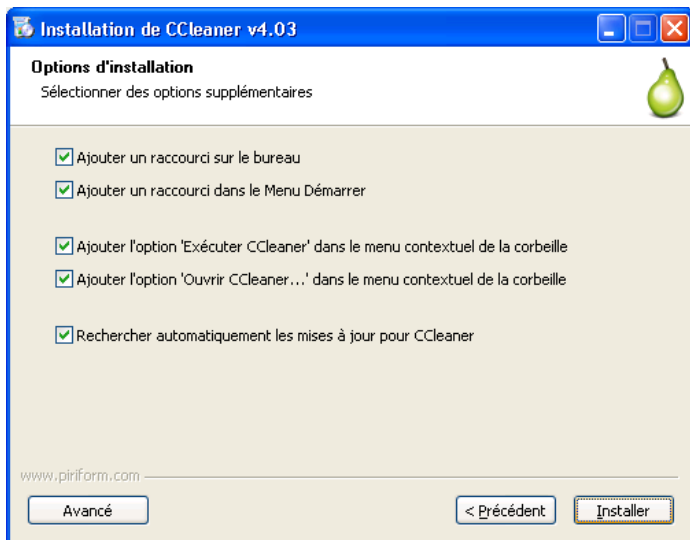



Figure 2: La fenêtre sans titre d'installation de Google Chrome défini comme navigateur par défaut

**Troisième étape.** Cliquez sur *Installer Google Chrome* en le définissant comme navigateur par défaut comme présenté ci-dessus pour l'empêcher de s'installer automatiquement sur votre ordinateur. Notez que cette fenêtre peut ne pas apparaître au cours de votre installation.

**Quatrième étape.** Cliquez sur  pour activer la fenêtre *Installation en cours* affichant la barre d'état de progression de l'installation.

**Cinquième étape.** Cliquez sur  pour finaliser l'installation de **CCleaner** et activer le message pop-up suivant :

Figure 3: Le message pop-up proposant le scanner intelligent de cookies

**Sixième étape.** Cliquez sur **NON** pour éviter de stocker des cookies en permanence sur votre ordinateur et activer l'interface utilisateur de *Piriform CCleaner*.

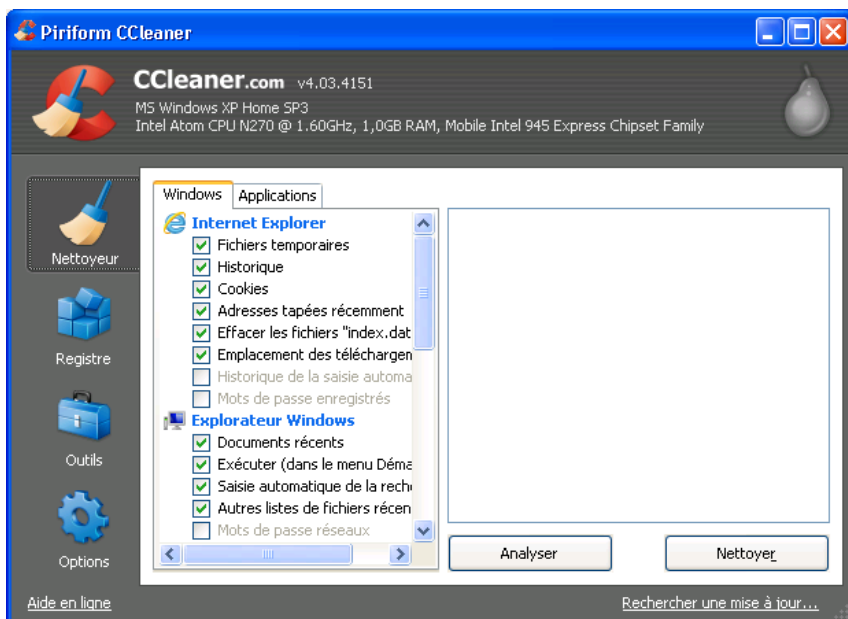


Figure 4: L'interface utilisateur de Piriform CCleaner

## 2.1 Avant de commencer à configurer CCleaner

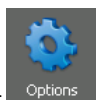
Tel que décrit en détail dans le chapitre 6. **Détruire définitivement des données sensibles** <sup>[37]</sup> du Livret pratique, les méthodes standard de suppressions de fichiers de **Microsoft Windows** ne suppriment pas réellement les données du disque (et ce, même lorsque vous videz votre "Corbeille"). *Même chose pour les fichiers temporaires. Pour supprimer ces fichiers de façon permanente du disque dur (ce qu'on appelle "nettoyer ou effacer le disque), il faut écraser les données en question avec des données aléatoires. CCleaner doit être configuré pour écraser les fichiers qu'il supprime et ainsi les nettoyer de façon sécuritaire, le programme n'est pas réglé de cette façon par défaut. CCleaner peut également supprimer de vieilles données inutiles en nettoyant l'espace libre de votre disque dur (veuillez consulter la section 5.3 Comment nettoyer l'espace disque libre avec CCleaner).*

## 2.2 Comment configurer CCleaner

Avant de commencer à utiliser **CCleaner**, vous devriez le régler pour être en mesure de supprimer les fichiers temporaires de façon permanente et sécuritaire.

Pour configurer CCleaner, suivez les étapes suivantes:

**Première étape.** Cliquez sur  ou sélectionnez Démarrer > Programmes > CCleaner pour afficher l'interface principale de Piriform CCleaner.



**Deuxième étape.** Cliquez sur  pour afficher la fenêtre suivante:

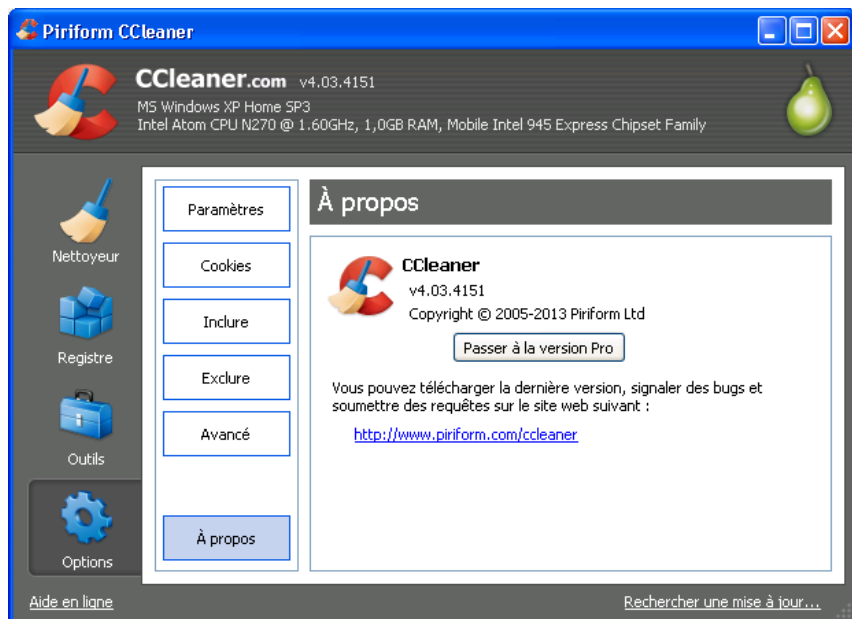
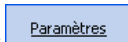


Figure 5: L'onglet Options affichant le panneau À propos par défaut

**Troisième étape.** Cliquez sur  pour afficher le panneau Paramètres. Le panneau Paramètres vous permet de choisir votre langue de travail et de déterminer comment CCleaner supprimera les fichiers temporaires et nettoiera vos disques.

**Commentaire:** La section *Effacement sécurisé* s'affiche avec l'option *Effacement normal de fichiers* sélectionnée par défaut.

**Quatrième étape.** Cliquez sur l'option *Effacement sécurisé (Lent)* pour activer le menu déroulant.

**Cinquième étape.** Développez le menu déroulant d'*Effacement sécurisé de fichiers* et sélectionnez l'item *Écrasement avancé* (3 passages) comme dans la fenêtre suivante:

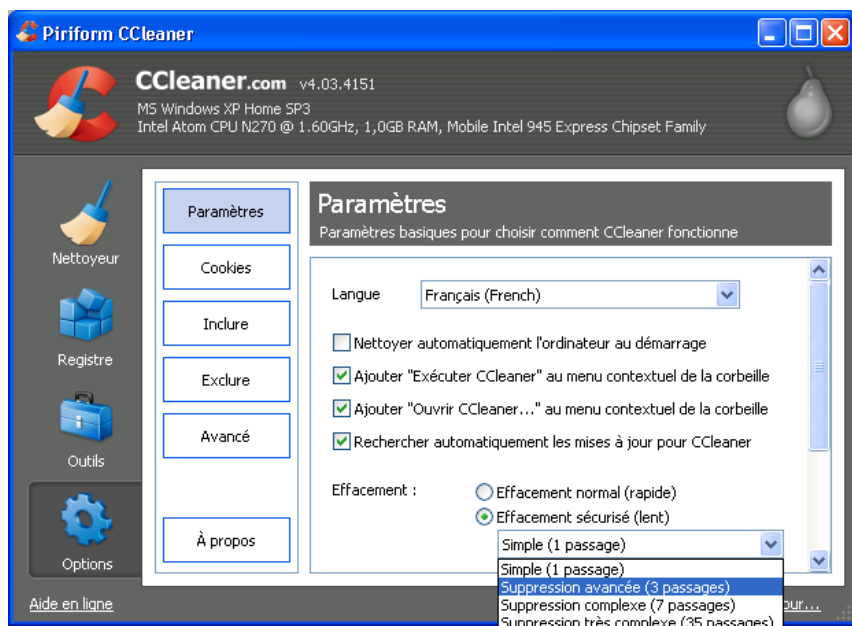


Figure 6: Le panneau Paramètres affichant les options d'Effacement sécurisé

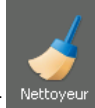
Après avoir configuré cette option, **CCleaner** écrasera les fichiers et dossiers que vous voulez supprimer avec des données aléatoires, ce qui les effacera de façon permanente. Les *Passages* du menu déroulant *Effacement sécurisé* réfère au nombre de fois que les données à effacer seront écrasées par des données aléatoires. Plus le nombre de passages est élevé, plus vos documents, fichiers ou dossiers seront écrasés avec des données aléatoires. Cela réduit considérablement la possibilité de restaurer ces documents, fichiers ou dossiers, mais cela augmente le temps de traitement requis par le processus d'effacement.

# Comment supprimer vos fichiers temporaires avec CCleaner

## 3.0 Comment supprimer vos fichiers temporaires

Dans cette section, nous verrons comment supprimer tous les fichiers temporaires générés par **Microsoft Windows** et la plupart des applications que vous utilisez sur votre ordinateur.

**Première étape.** Cliquez sur  ou sélectionnez **Démarrer > Programmes > CCleaner** pour afficher la fenêtre principale de **CCleaner**.



**Deuxième étape.** Cliquez sur  pour afficher la fenêtre suivante:

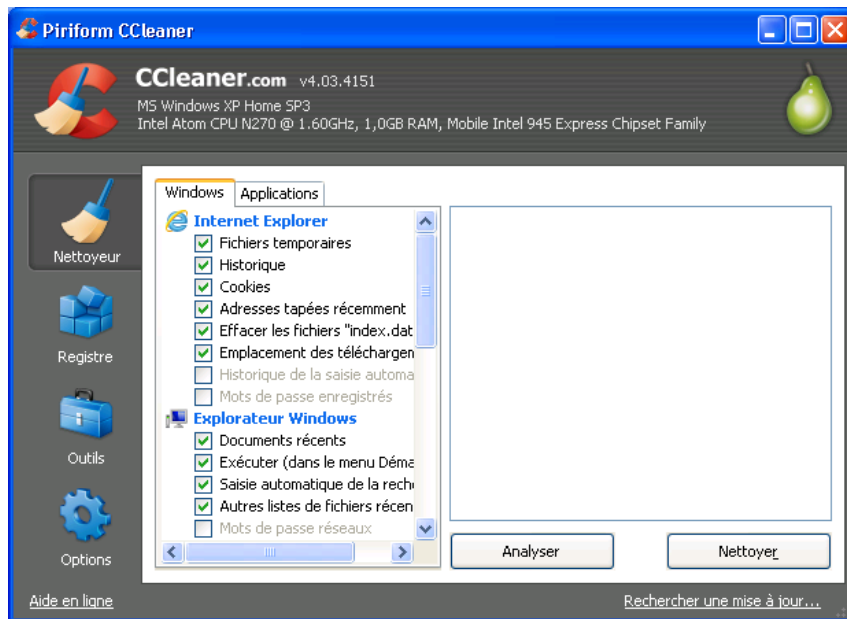


Figure 1: L'interface principale de CCleaner affichant la fenêtre Nettoyeur

La fenêtre *Nettoyeur* est divisée en deux panneaux: le panneau de gauche présente les onglets *Windows* et *Applications*, et le panneau de droite est un espace vide où s'affichent l'information ou les résultats d'une opération de nettoyage donnée. Les boutons *Analyser* et *Nettoyer* se trouvent juste en dessous de cet espace.

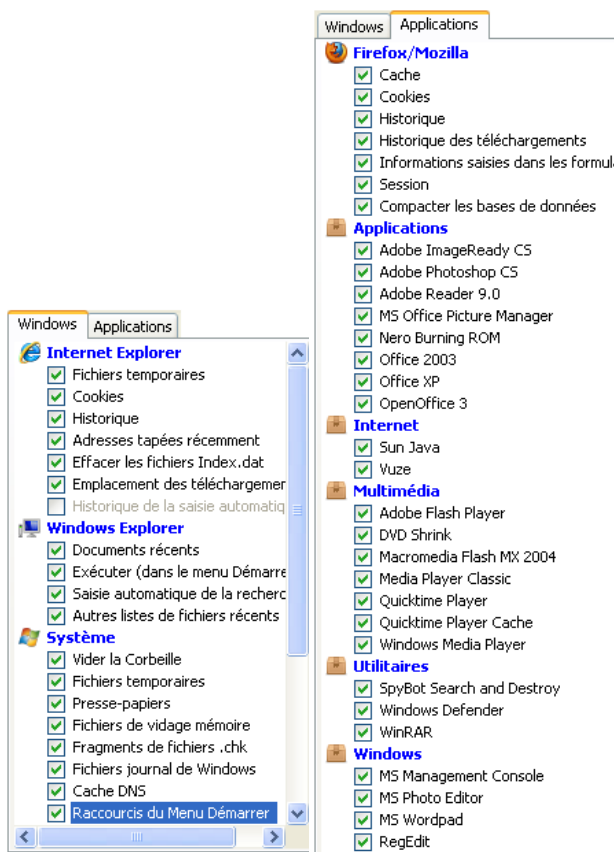


Figure 2: Les onglets Windows et Applications avec toutes les options cochées

**Commentaire:** En suivant les prochaines étapes, vous supprimerez les fichiers temporaires associés aux items que vous avez cochés dans les onglets *Windows* et *Applications*. Puisque différents utilisateurs ont différents logiciels installés sur leurs ordinateurs, votre propre liste d'applications peut être assez différente de celle que présente la *Figure 2* ci-dessous.

**Troisième étape:** Faites défiler les onglets *Windows* et *Applications* et **cochez** toutes les options de la section *Avancé* également. En cochant certaines options, une boîte de dialogue de confirmation s'affiche pour expliquer ce qu'implique chaque option:

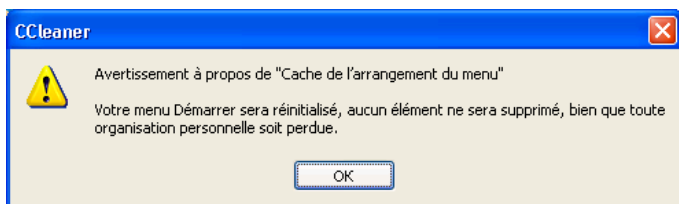


Figure 3: Un exemple de boîte de dialogue de confirmation

**Attention:** En cochant l'option *Nettoyage de l'espace libre*, vous allez considérablement augmenter la quantité de temps nécessaire au processus de nettoyage. De ce fait, assurez-vous que vous disposez d'une heure ou plus pour effectuer ceci.

**Commentaire:** **Cochez** toutes les options des des onglets *Windows* et *Applications* pour permettre un nettoyage complet et rigoureux des fichiers temporaires. Il est cependant important que vous compreniez bien quels types de réglages et de paramètres sont supprimés. **Cliquez** sur  pour fermer tous les messages et poursuivre le processus de suppression des fichiers temporaires.

**Quatrième étape.** Cliquez sur  pour générer une liste de tous les fichiers temporaires pouvant être supprimés.

**Astuce:** Fermez tous les autres programmes avant d'entamer le processus de nettoyage. Si vous les laissez activés, **CCleaner** ne pourra peut-être pas supprimer tous les fichiers temporaires associés à ces programmes, et il est possible que vous receviez des avertissements comme celui-ci:

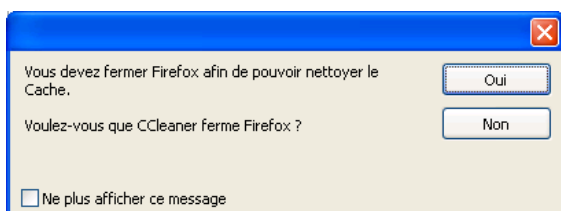


Figure 4: Un exemple de message d'avertissement de fermer Firefox/Mozilla

Cinquième étape. Cliquez sur  pour poursuivre l'analyse.

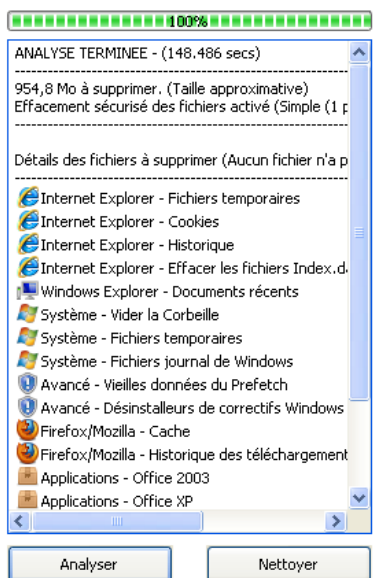


Figure 5: Un exemple de liste de fichiers temporaires pouvant être supprimés

**Commentaire:** CCleaner supprime les fichiers temporaires générés lorsque vous utilisez une application, mais *ne supprime pas* l'application elle-même. Dans la Figure 5, par exemple, la suite de programmes *Applications - Office 2003* reste installée sur l'ordinateur, mais les fichiers temporaires générés par ce programme sont supprimés. Pour désinstaller des programmes à l'aide de CCleaner, veuillez vous référer à la section [Options avancées, FAQ et questions récapitulatives](#) [124], [5.1 Comment désinstaller des programmes avec CCleaner](#).

Sixième étape. Cliquez sur  pour activer la fenêtre suivante :

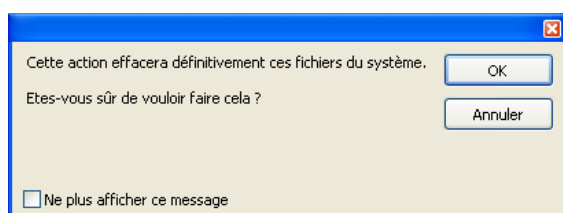


Figure 6: Boîte de dialogue de confirmation

Septième étape. Cliquez sur  pour supprimer ces fichiers temporaires. Lorsque le processus de suppression est complété, le résultat s'affiche comme suit:



Figure 7: Le résultat de la suppression de fichiers temporaires

Vous avez réussi à supprimer les fichiers temporaires de *Windows* et de vos *Applications* avec CCleaner.

## Comment nettoyer le Registre de Windows avec CCleaner

Sommaire des sections de cette page:



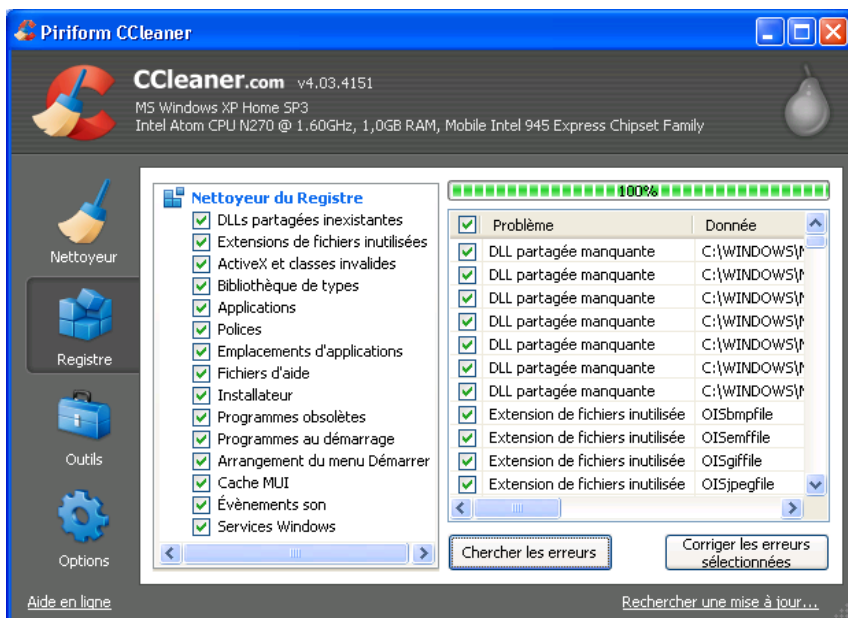


Figure 2: La panneau des résultats affichant une liste de problèmes à corriger

En guise de mesure de précaution avant de corriger le **Registre Windows**, le programme vous proposera de créer une copie de sauvegarde du registre. Si un quelconque problème survient suite au nettoyage du **Registre de Windows**, il vous sera possible de restaurer le **Registre de Windows** à son état précédent en utilisant cette copie de sauvegarde.

**Troisième étape.** Cliquez sur  pour afficher la boîte de dialogue de confirmation illustrée ci-dessous:

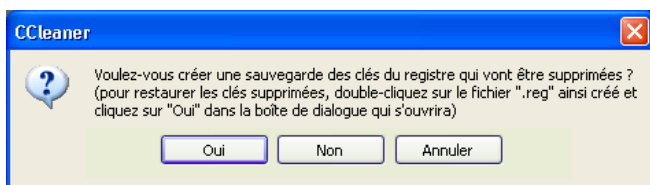


Figure 3: La boîte de dialogue de confirmation

**Astuce:** Si vous oubliez l'emplacement de votre copie de sauvegarde, vous n'avez qu'à effectuer une recherche de l'extension de fichier `.reg`.

**Quatrième étape.** Cliquez sur  pour créer une copie de sauvegarde des clés du registre et afficher la fenêtre suivante:

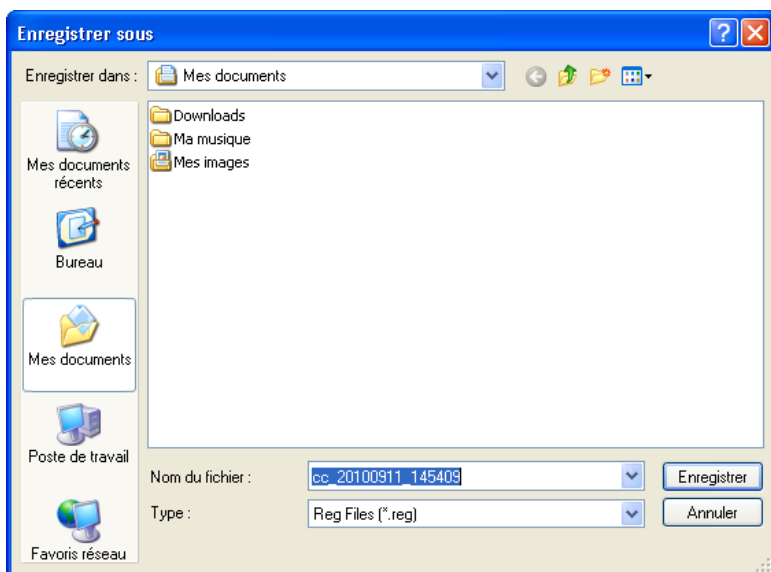


Figure 4: La fenêtre Enregistrer sous

**Cinquième étape.** Cliquez sur , après avoir choisi un emplacement pour votre copie de sauvegarde, pour afficher la fenêtre suivante:



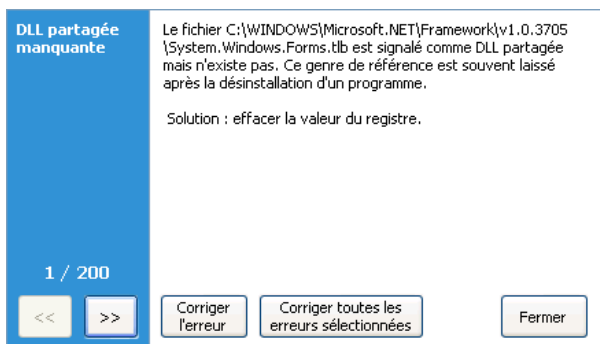



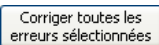


Figure 5: La boîte de dialogue Corriger l'erreur/Corriger toutes les erreurs sélectionnées

**Commentaire:** Les utilisateurs experts ou avancés apprécieront la possibilité de corriger certaines erreurs et d'en ignorer d'autres, selon leur préférences. Il est recommandé aux utilisateurs moyens ou intermédiaires de corriger toutes les erreurs sélectionnées.

**Sixième étape.** Cliquez sur  ou  pour afficher chaque erreur, puis cliquez sur  pour corriger uniquement celles que vous souhaitez corriger.

**Septième étape.** Cliquez sur  pour corriger toutes les erreurs sélectionnées et cliquez sur **Fermer** pour achever le processus de nettoyage.

**Astuce:** Répétez les **étapes 2 à 7** jusqu'à ce qu'il n'y ait plus aucune erreur à corriger.

Le **Registre de Windows** a été nettoyé avec succès.

## 4.2 Comment restaurer un fichier de sauvegarde du registre

Si vous avez l'impression que le nettoyage du **Registre de Windows** a occasionné un problème avec le fonctionnement normal de votre système, le fichier de sauvegarde que vous avez créé aux **étapes 3 à 5** de la section **4.1** peut être utilisé pour restaurer le registre à son état précédent et ainsi réduire l'interférence avec votre système.

Pour restaurer le registre, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez **Démarrer > Exécuter** pour afficher la boîte de dialogue *Exécuter*, puis saisissez *regedit*, comme suit:

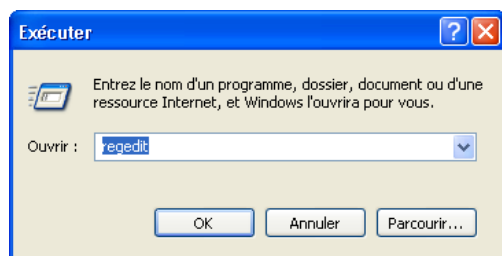
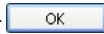


Figure 6: La boîte de dialogue Exécuter

**Deuxième étape.** Cliquez sur  pour afficher la fenêtre suivante:

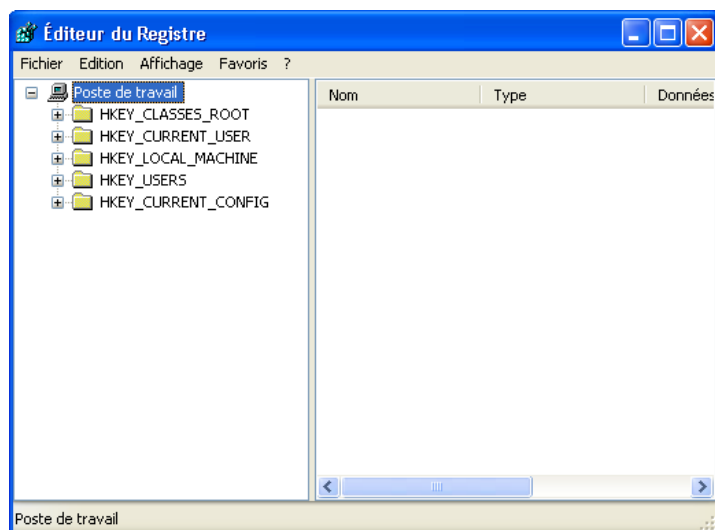



Figure 7: L'Éditeur du registre

**Troisième étape.** Sélectionnez **Fichier > Importer** dans la barre de menu pour afficher la fenêtre *Importer un fichier du registre*, puis sélectionnez  cc\_20100911\_145409.

Quatrième étape. Cliquez sur  pour afficher la boîte de dialogue suivante:

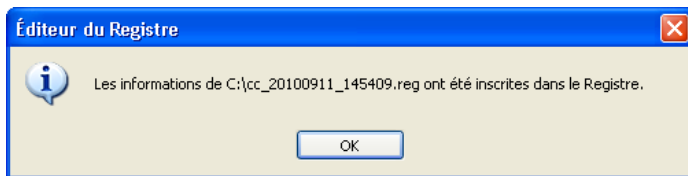


Figure 8: Une autre Boîte de dialogue de l'Éditeur du registre confirmant que le fichier de sauvegarde a été restauré

Cinquième étape. Cliquez sur  pour finaliser la restauration du fichier de sauvegarde du registre.

## Options avancées, faq et questions récapitulatives

Sommaire des sections de cette page:

- [5.0 Options avancées](#)
- [5.1 Comment désinstaller des programmes avec CCleaner](#)
- [5.2 Comment désactiver le lancement au démarrage des programmes avec CCleaner](#)
- [5.3 Comment nettoyer l'espace libre de vos disques durs avec CCleaner](#)
- [5.4 Faq](#)
- [5.5 Questions récapitulatives](#)

### 5.0 Options avancées

Deux autres fonctions de **CCleaner** peuvent améliorer considérablement l'efficacité générale de votre système: les fonctions *Désinstallation de programmes* et *Démarrage*. Ces fonctions sont décrites dans les sections suivantes. Vous apprendrez également comment *Nettoyer*, ou *Effacer*, l'espace libre de vos disques durs.

### 5.1 Comment désinstaller des programmes avec CCleaner

**Important:** Assurez-vous que le programme à supprimer ou désinstaller n'est pas essentiel au bon fonctionnement de votre ordinateur.

En supprimant des logiciels préalablement installés, qui sont désormais inutilisés ou superflus, avant de lancer **CCleaner**, il est possible que vous en supprimiez également les fichiers temporaires. Cela peut réduire le nombre de fichiers et dossiers temporaires à supprimer, ainsi que la durée du processus de nettoyage.

La fonction *Désinstallation de programmes* de **CCleaner** est semblable à la fonction **Ajout/Suppression de programmes** de **Microsoft Windows**. La fonction **\*\* Désinstallation de programmes\*\*** liste les programmes plus clairement et plus rapidement.

Pour entamer la désinstallation des programmes obsolètes, suivez les étapes énumérées ci-dessous:

**Première étape.** Cliquez sur  ou sélectionnez **Démarrer > Programmes > CCleaner** pour activer l'interface principale de *Piriform CCleaner*.



**Deuxième étape.** Cliquez sur , puis cliquez sur  pour afficher la fenêtre ci-dessous:

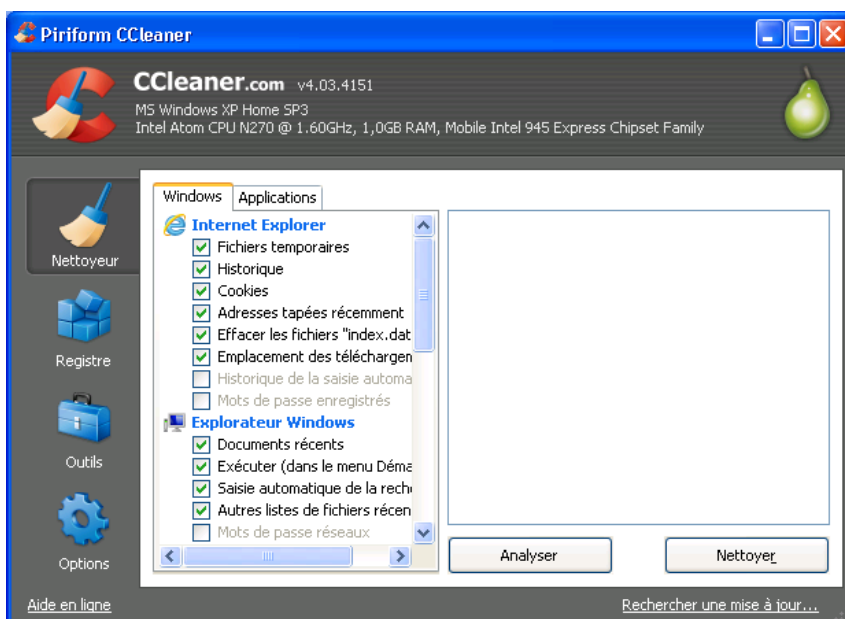
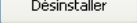




Figure 1: L'option Outils affichant le panneau Désinstallation de programmes

Troisième étape. Sélectionnez un programme dans la liste *Programmes*, puis cliquez sur  pour désinstaller le programme sélectionné.

**Astuce:** Les utilisateurs avancés ou experts trouveront sans doute les fonctions *Renommer l'entrée* et *Effacer l'entrée* utiles pour garder confidentielle l'existence de certains logiciels. Ces deux fonctions vous assurent que personne d'autre que vous ne puisse détecter l'existence de ce programme, ce qui le protège des parties potentiellement hostiles ou malveillantes qui pourraient utiliser la fonction **Ajout/Suppression de programmes** de **Microsoft Windows** ou celle de **CCleaner** pour les afficher.

Cliquez sur  pour renommer le programme. Autrement, vous pouvez cliquer sur  pour supprimer le programme de la liste, mais *sans pour autant* le supprimer

## 5.2 Comment désactiver le lancement au démarrage des programmes avec CCleaner

Un programme lancé au démarrage est réglé pour se lancer automatiquement lorsque vous allumez votre ordinateur. Les programmes lancés automatiquement peuvent être exigeants envers les ressources limitées du système et ainsi ralentir l'ordinateur au démarrage.

 Première étape. Cliquez sur , puis cliquez sur  pour afficher la fenêtre suivante:

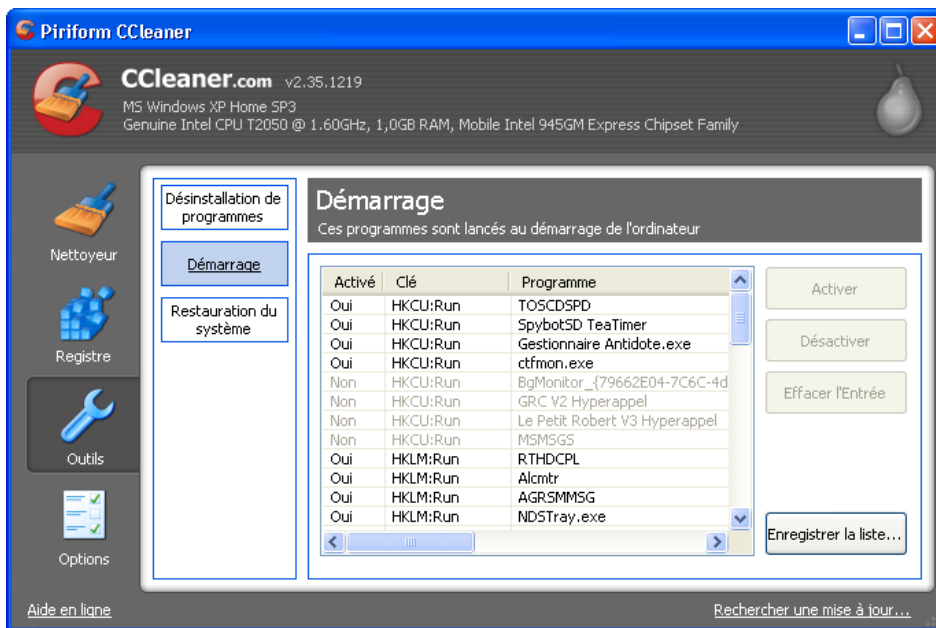
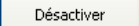


Figure 12: L'option *Outils* affichant le panneau *Démarrage*

Deuxième étape. Sélectionnez un programme dans la liste du panneau *Démarrage*, puis cliquez sur  pour désactiver le lancement au démarrage du programme.

## 5.3 Comment nettoyer l'espace libre de vos disques durs avec CCleaner

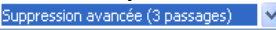
Dans le système d'exploitation **Windows**, la suppression d'un fichier ne fait que supprimer la référence à ce fichier sans supprimer les données elles-mêmes. Bien que l'espace occupé par ces données sur le disque sur lequel sera éventuellement écrasé par d'autres fichiers, une personne experte pourrait être en mesure de reconstruire le fichier en partie ou en entier. Cependant, vous pouvez empêcher cela en nettoyant, ou effaçant, l'espace libre de votre disque dur. **CCleaner** vous permet également de nettoyer la **Master File Table (MFT)**.




La **Master File Table (MFT)** est un index de tous les noms de fichier, leur emplacement et autres renseignements connexes. Lorsque **Microsoft Windows** supprime un fichier, le système marque ce fichier comme 'supprimé' uniquement pour des raisons de rendement. L'entrée **MFT** du fichier, ainsi que le contenu du fichier, demeure sur le disque dur.

**Commentaire:** Le nettoyage du disque dur et de la **MFT** requiert une somme considérable de temps, et le temps requis dépend du nombre de passages déterminé.

Avant d'entamer le nettoyage de l'espace libre du disque dur et de la **MFT**, certaines options doivent être réglées dans les panneaux *Options* > *Paramètres* et *Nettoyeur*.

Pour choisir le disque que vous souhaitez nettoyer, suivez les étapes énumérées ci-dessous:

Première étape. Faites dérouler la liste vers le bas et cochez l'option *Effacement sécurisé (lent)*, puis sélectionnez  si cela n'est pas déjà fait.

 Deuxième étape. Cliquez sur , puis sur  pour afficher le panneau *Paramètres*.

**Troisième étape. Cochez** les options *Lecteurs sur lesquels nettoyer l'espace libre* et *Nettoyer l'espace libre de la MFT*, tel qu'illustré ci-dessous:

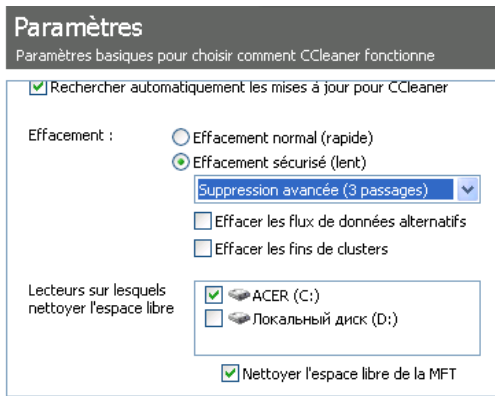


Figure 3: Le panneau Paramètres avec les deux options de nettoyage sélectionnés



**Quatrième étape. Cliquez** sur **Nettoyeur** pour afficher l'interface principale de Piriform CCleaner.

**Commentaire:** La prochaine étape est optionnelle si vous avez déjà activé cette option lorsque vous avez exécuté un nettoyage de routine de vos fichiers temporaires.

**Astuce:** Souvenez-vous de fermer tous les programmes ouverts avant de lancer le processus de nettoyage. Si laissez certains programmes ouverts, **CCleaner** ne sera peut-être pas en mesure de supprimer tous les fichiers temporaires qui y sont associés.

**Cinquième étape. Faites dérouler** l'onglet *Windows* vers le bas jusqu'à la section *Avancé*, puis **cochez** l'option *Nettoyer l'espace libre* pour afficher la fenêtre d'avertissement ci-dessous:

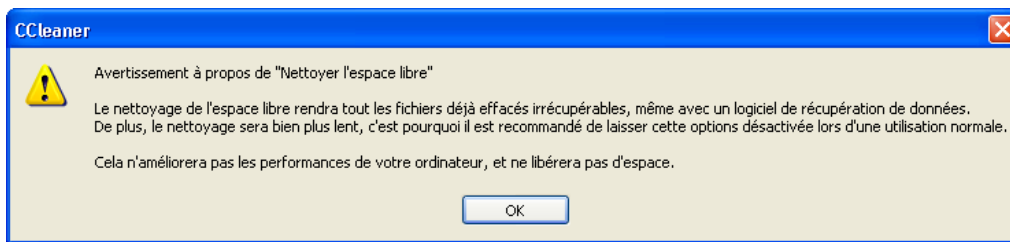


Figure 4: La boîte de dialogue d'avertissement

**Sixième étape. Cliquez** sur **OK**, puis **cliquez** sur **Nettoyer** pour afficher la fenêtre suivante:

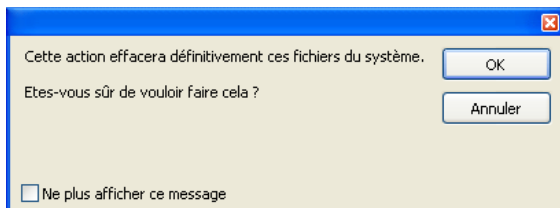


Figure 5: La boîte de dialogue de confirmation

**Septième étape. Cliquez** sur **OK** pour entamer le nettoyage de l'espace libre de votre disque dur, et de la **Master File Table**.

## 5.4 Faq

Elena et Nikolai trouvent **CCleaner** facile à utiliser, mais ils ont encore quelques questions sur son emploi:

**Q:** Si je désinstalle **CCleaner**, est-ce que le matériel que j'ai supprimé restera effacé?

**A:** Oui. Si tu as configuré et utilisé **CCleaner** adéquatement, les fichiers supprimés sont éliminés définitivement.

**Q:** Si je sauvegarde **CCleaner** sur ma clé USB, puis-je l'utiliser sur l'ordinateur d'un café Internet pour effacer les traces du travail que j'y ai effectué ? Y a-t-il une raison pour laquelle je ne devrais pas l'utiliser de cette façon?

**A:** Oui! Il existe une version portable de **CCleaner**. Il faut consulter la section **CCleaner - Portable** de la page de téléchargement [www.piriform.com/ccleaner/builds](http://www.piriform.com/ccleaner/builds) [118]. Si le café Internet te permet d'exécuter des programmes à partir d'une clé USB, alors oui, il est possible d'utiliser **CCleaner** pour effacer les traces du travail que tu as effectué sur cet ordinateur. Par contre, n'oublie pas que ton activité au café Internet est peut-être contrôlée. De plus, tu risques d'infecter ta clé USB en la connectant à l'ordinateur du café Internet.

**Q:** Si je n'utilise qu'un seul passage de **CCleaner**, est-ce qu'une autre personne sera en mesure de récupérer mes

données? Et si j'en utilise sept?

**A:** Excellente question! Plus le nombre de passages exécutés est élevé pour effacer des données, moins il y a de chance qu'une tierce personne ne les récupère : cependant, le processus de nettoyage sera plus long.

**Q:** Si je nettoie le **Registre de Windows**, est-ce que toutes les traces des programmes que j'ai temporairement chargés sur mon ordinateur et ensuite enlevés seront effacés?

**A:** Oui. Tu devrais aussi effectuer le nettoyage des fichiers temporaires en plus de nettoyer le **Registre de Windows**. Ainsi, tu effaceras toute trace de logiciels (et du coup, des opérations que tu y as faites) qui n'existent plus sur ton ordinateur. Cependant, si tu n'a que très peu de temps, le nettoyage du **Registre de Windows** est un bon départ!

## 5.5 Questions récapitulatives

- Quelle information CCleaner efface-t-il de votre ordinateur?
- Comment procède-t-il?
- Quelle différence y a-t-il entre le nombre de passes que vous choisissez au moment d'écraser des données de façon sécuritaire?
- Qu'est-ce que le **Registre de Windows**, et pourquoi est-il recommandé de le nettoyer?
- Que devriez-vous faire avant de nettoyer **Registre de Windows**?

# Riseup - service de courriel sécurisé

## Short Description:

**RiseUp** est un collectif dont l'objectif premier est d'offrir des services d'hébergement Web, de listes de distribution et de courrier électronique privés et sécurisés à des individus et organismes qui luttent pour la justice sociale.

## Site Internet

<https://riseup.net/> <sup>[125]</sup>

## Configuration requise

- Une connexion Internet
- **RiseUp** offre une fonctionnalité accrue avec le navigateur **Firefox**

## Licence

- Gratuitiel (*Freeware*)

## Lecture préalable

- Livret pratique Security in-a-box, chapitre **7. Préserver la confidentialité de vos communications sur Internet** <sup>[126]</sup>

**Niveau:** 1 : Débutant, 2 : **Moyen**, 3 : Intermédiaire, 4 : Expérimenté, 5 : Avancé

**Temps d'apprentissage:** 20 minutes

## Ce que vous apportera l'utilisation de cet outil:

- L'accès à un compte de courrier électronique sans publicité, autogéré par une communauté militante.
- La possibilité d'accéder à votre courrier électronique par Internet ou à l'aide d'un client de messagerie, et de communiquer confidentiellement par courrier électronique via une connexion chiffrée.
- La capacité de modifier votre adresse de courriel, de déterminer la taille de votre boîte de courriel et d'inviter d'autres personnes à joindre **RiseUp**

## Autres services de courrier électronique:

Même si **RiseUp** offre un service sécurisé, géré par un collectif de confiance qui accorde beaucoup d'importance à la sécurité numérique, un service de courrier électronique inhabituel pourrait attirer une attention non désirable. Dans certaines situations, il peut être plus avantageux de passer inaperçu en optant plutôt pour un service de courriel populaire dans votre pays. L'important est de prendre une décision éclairée sans compromettre vos besoins élémentaires en matière de sécurité. Voici quelques considérations à tenir en compte lorsque vous choisissez un service de courrier électronique:

1. Le service permet-il d'utiliser des canaux chiffrés (comme *https*, et d'autres versions chiffrées SSL des protocoles comme IMAP, POP3 et SMTP) pour transférer l'information (y compris les détails de connexion et le contenu des messages); et le service présente-t-il des problèmes de chiffrement (par exemple, des problèmes liés aux certificats de chiffrement)?
2. Les serveurs de courriel sont-ils gérés de façon sûre et sécuritaire? Sont-ils gérés par des professionnels qui emploient les pratiques exemplaires pour protéger vos données? Leur faites-vous confiance pour *ne pas* donner l'accès à vos données, pour quelque raison que ce soit (commerciale, politique, religieuse, etc.), à des tierces parties?
3. Connaissez-vous l'emplacement géographique des serveurs; sous quelle juridiction territoriale se trouvent-ils; ou dans quel pays la compagnie est-elle située? Savez-vous de quelle façon ces renseignements peuvent avoir un impact sur la confidentialité et la sécurité de vos communications par courrier électronique?

Dans certaines parties du monde, **Google Mail** peut s'avérer une bonne alternative à **RiseUp**, puisque ce service est très répandu et permet de passer inaperçu sans pour autant compromettre la sécurité de vos communications (étant donné son caractère commercial).

## 1.1 À propos de cet outil

**RiseUp** est un collectif dont l'objectif premier est d'offrir des services d'hébergement Web, de listes de distribution et de courrier électronique privés et sécurisés à des individus et organismes qui luttent pour la justice sociale. Puisque leurs services sont gratuits, les comptes de courriel offerts par **RiseUp** sont considérablement plus petits que ceux qu'offrent les fournisseurs de services non sécurisés et/ou soumis aux intérêts publicitaires. De plus, un nouveau compte ne peut être enregistré que par une personne qui a reçu des codes d'invitation de la part de membres existants ou de participants au projet **Digital Security**.

**RiseUp** fonctionne exclusivement avec le protocole **Secure Sockets Layer (SSL)**, ce qui assure une connexion sécurisée entre votre ordinateur et leur serveur. Ce niveau de sécurité est maintenu lorsque vous relevez votre courrier électronique à l'aide d'un client de messagerie, avec une connexion sécurisée utilisant **POP**, **IMAP** ou **SMTP** (différents protocoles spéciaux utilisés par des programmes de messagerie pour télécharger votre courrier électronique).

**RiseUp** est compatible avec **Mozilla Thunderbird**. Pour apprendre à configurer **Mozilla Thunderbird** pour accéder à votre compte **RiseUp**, veuillez consulter le Guide pratique **Thunderbird** <sup>[127]</sup>.

## Comment créer un compte Riseup

Sommaire des sections de cette page:

- [2.0 Les différentes méthodes d'enregistrement d'un compte RiseUp](#)
- [2.1 Le formulaire d'Information sur le compte](#)
- [2.2 Le formulaire de Mot de passe](#)
- [2.3 Le formulaire d'Entraide](#)
- [2.4 Le formulaire d'Activation](#)

---

## 2.0 Les différentes méthodes d'enregistrement d'un compte RiseUp

**RiseUp** offre trois méthodes différentes pour enregistrer un compte de courriel. Chaque méthode exige un investissement variable de temps et d'effort.

1) Des individus et/ou des organismes sont invités par deux personnes disposant déjà de comptes **RiseUp**. Cette méthode implique que vous receviez un code d'invitation de la part de chacune de ces personnes. Pour savoir comment ces codes sont générés, consultez la section [4.3 La page Invitations](#) <sup>[128]</sup>

2) Effectuer une demande directement à l'équipe **RiseUp** pour obtenir un compte. Cette méthode exige beaucoup de patience. N'oubliez pas que **RiseUp** repose principalement sur l'enthousiasme et la bonne volonté de ses bénévoles!

3) Les participants au programme de formation du **Digital Security Project** recevront un code d'enregistrement avec leur copie de la trousse à outils **Security in-a-box**.

Après avoir reçu vos codes d'invitation, suivez les étapes énumérées ci-dessous pour enregistrer votre compte **RiseUp** gratuit :

**Première étape.** Saisissez <https://mail.riseup.net> <sup>[129]</sup> dans la barre d'adresse de votre navigateur pour activer le site Internet de **RiseUp**, illustré ci-dessous:

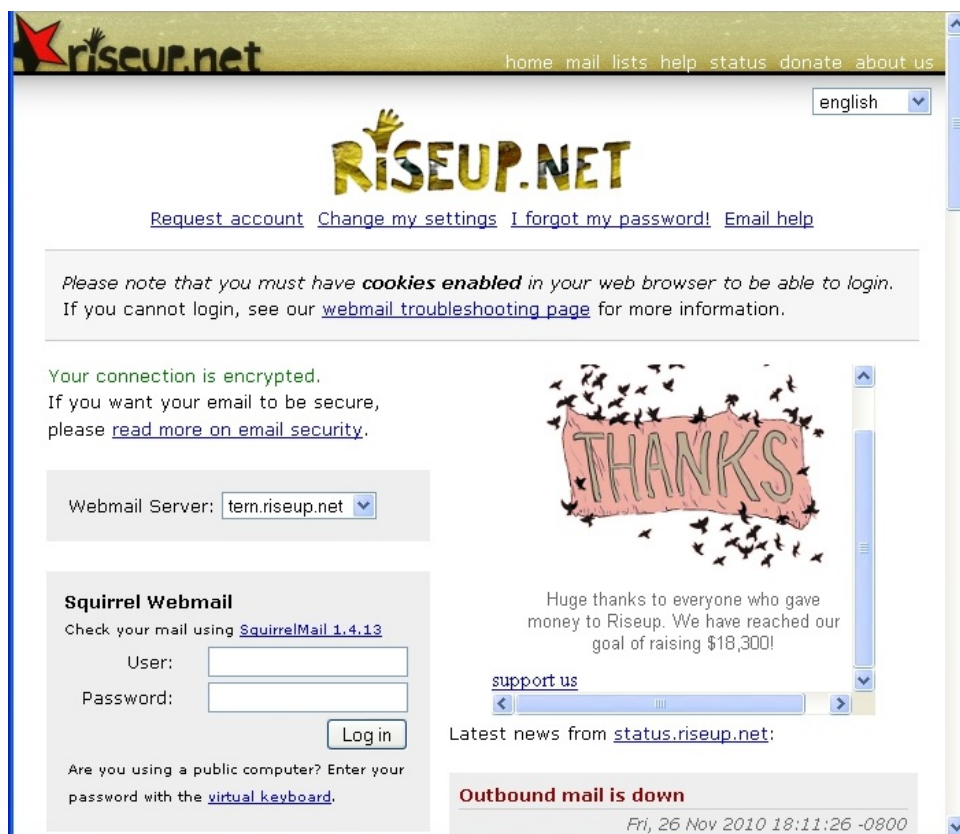


Figure 1: La page <https://mail.riseup.net/>

**Commentaire:** Le **s** dans l'adresse <https://> Cela indique que vous communiquez via une connexion *Secure Socket Layer* (SSL), et le message texte en vert *Your connection is encrypted* est affiché au dessus des zones de texte servant à la connexion.

Pour plus de renseignements à ce sujet, veuillez consulter le chapitre **7. Préserver la confidentialité de vos communications sur Internet** <sup>[126]</sup> du **livret pratique**, ou visitez <https://help.riseup.net/security> <sup>[130]</sup>.

**Deuxième étape.** Cliquez sur [Request account](#) pour afficher la page *Demander un nouveau compte* illustrée ci-dessous :

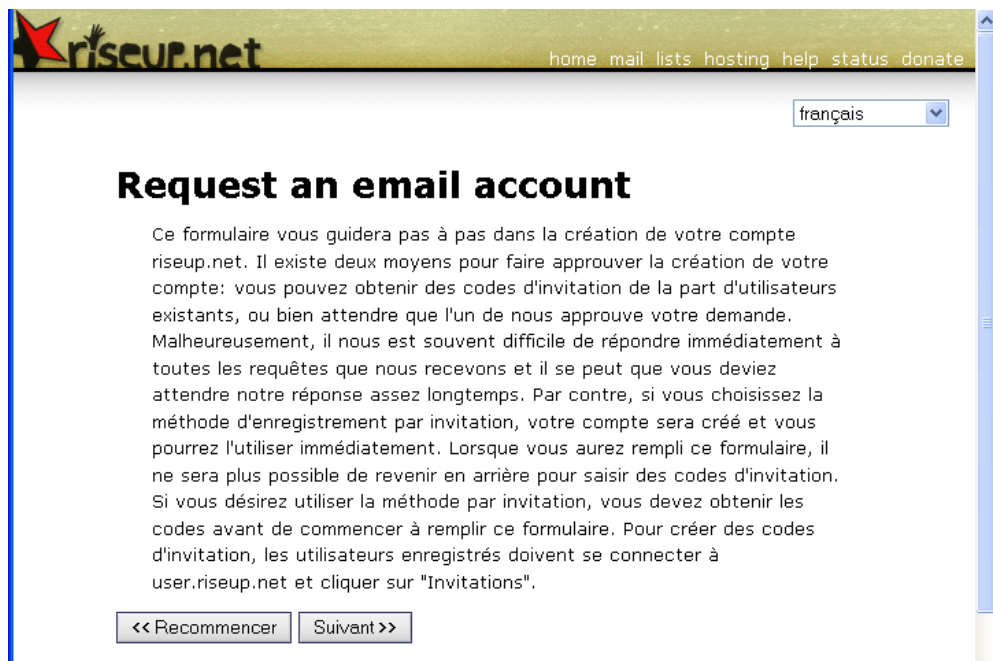


Figure 2: La page *Demander un nouveau compte* de RiseUp

**Étape optionnelle.** Sélectionnez votre langue d'usage dans le menu défilant qui se trouve à droite de l'écran, si nécessaire.

**Troisième étape.** Cliquez sur  pour afficher la page **RiseUp À propos de notre service de courriel**.

**Important:** Vous devez cocher les options suivantes afin de poursuivre le processus de création d'un compte **RiseUp**.

**Quatrième étape.** Après avoir lu les politiques de **RiseUp**, **cochez** les options *J'accepte le contrat social de riseup.net*, *J'accepte la politique de confidentialité de riseup.net* et *J'accepte les termes d'utilisation de riseup.net*.

**Cinquième étape.** Cliquez sur  pour commencer à créer votre compte **RiseUp** en remplissant les formulaires : *Information sur le compte*, *Mot de passe*, *Entraide* et *Activation*.

## 2.1 Le formulaire d'Information sur le compte

**Sixième étape.** Saisissez un nom d'utilisateur pour votre compte. Ce nom sera utilisé pour vous connecter au site et vous servira d'adresse de courriel (par exemple, saisissez le nom "thierryfictif" si vous souhaitez que votre adresse de courriel soit [thierryfictif@riseup.net](mailto:thierryfictif@riseup.net)).

**Important:** n'utilisez pas d'espace, de virgules ou de point final dans le nom d'utilisateur.

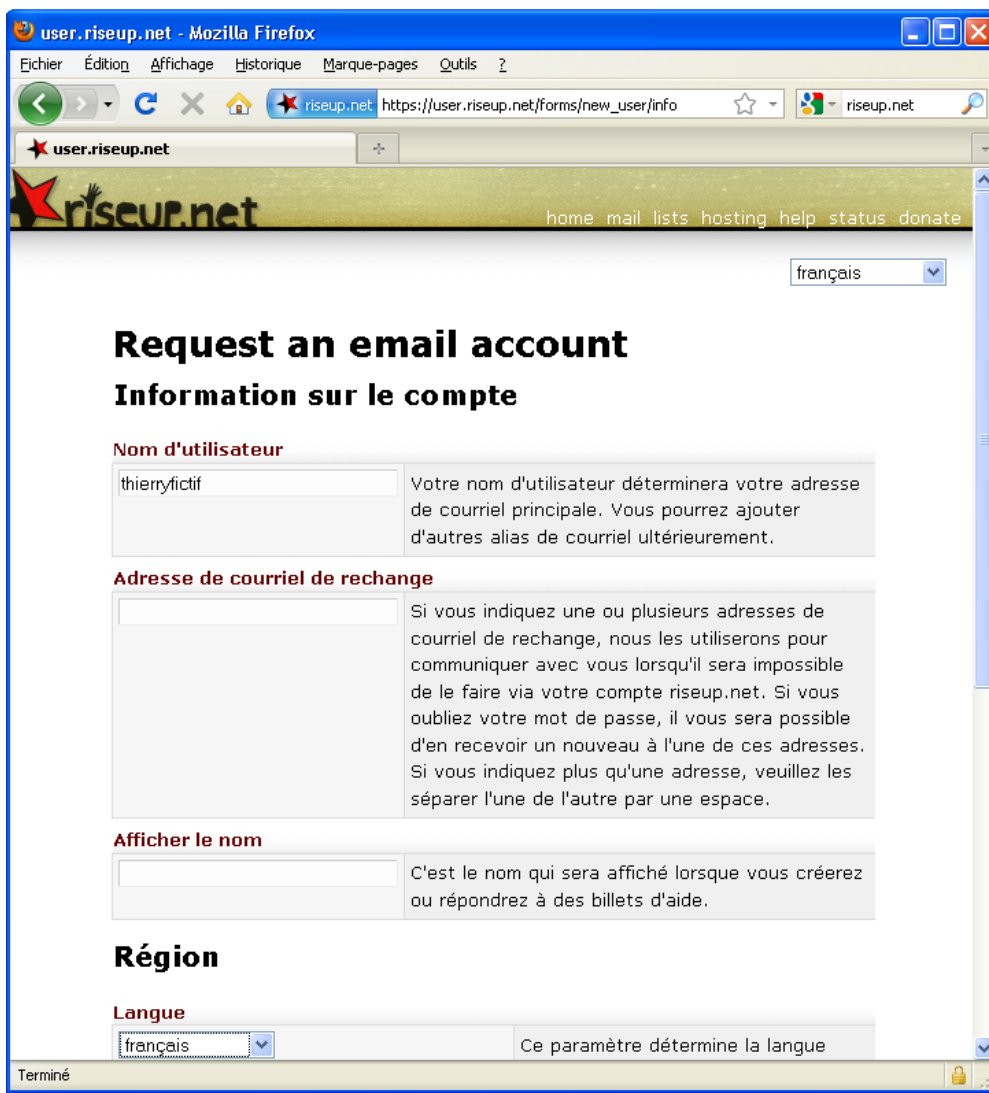


Figure 3: Un formulaire d'Information sur le compte dûment rempli

**Septième étape.** Cliquez sur  après avoir choisi un nom d'utilisateur original, pour afficher la page du formulaire *Mot de passe*.

**Commentaire:** Si ce nom d'utilisateur existe déjà, vous devrez en créer un nouveau.

## 2.2 Le formulaire de Mot de passe

Dans ce formulaire, vous devez créer une question de sécurité et la réponse assortie, ainsi qu'un bon mot de passe afin de protéger la connexion à votre compte, faute de quoi il ne vous sera pas permis de poursuivre le processus de création du compte. **RiseUp** vous recommande de créer une question de sécurité comme recours d'urgence au cas où vous oublieriez votre mot de passe. Malheureusement, cette mesure bien intentionnée constitue une vulnérabilité.

Par exemple, un adversaire potentiel n'aurait en théorie qu'à deviner la bonne réponse pour intercepter le nouveau mot de passe qui vous serait alors envoyé. Il est donc fortement *recommandé* d'éliminer complètement la possibilité de deviner la réponse à votre question secrète en *sabotant* ces deux zones de texte, tel qu'illustré dans l'exemple ci-dessous :



**Question secrète**

Quelle est votre couleur préférée?	Si vous oubliez votre mot de passe, il vous sera possible de le changer en répondant à cette question de mot de passe. C'est pourquoi il est important que vous choisissiez une question dont vous seul connaissez la réponse.
------------------------------------	--

**Réponse secrète**

dfm3qer87gvrigrb	Ceci est la réponse secrète à votre question de mot de passe.
------------------	---

**Anniversaire**

<input type="text"/> <input type="text"/>	Avant de pouvoir changer votre mot de passe en répondant à votre question secrète, vous devrez indiquer votre date d'anniversaire, telle que vous l'aurez saisie ici.
---	---

**Mot de passe**

<input type="text"/>	Saisissez votre mot de passe ici. Veuillez choisir un mot de passe comprenant au moins six caractères et une combinaison de lettres, de chiffres et de symboles.
----------------------	--

**Saisir le mot de passe de nouveau**

<input type="text"/>	Saisissez votre mot de passe de nouveau pour confirmer que vous n'avez pas fait d'erreur.
----------------------	---

<< Précédent    Suivant >>

Figure 4: Une exemple de question et réponse sabotées dans le formulaire de Mot de passe

**Attention:** Cela signifie également qu'il sera pratiquement impossible de réinitialiser votre mot de passe. Vous devrez vous en rappeler! Si cette méthode n'est pas vraiment pratique, ça demeure l'option la plus sûre.

Le mot de passe pour votre compte **RiseUp** est l'élément le plus important en ce qui à trait à la sécurité du comte. Vous devez choisir un mot de passe fort. Pour plus d'information à ce sujet, veuillez consulter le chapitre **3. Créer et sauvegarder des mots de passe sûrs** <sup>[54]</sup> du livret pratique, ainsi que le Guide pratique **KeePass** <sup>[82]</sup>.

**Mot de passe**

●●●●●●●●●●●●●●●●	Saisissez votre mot de passe ici. Veuillez choisir un mot de passe comprenant au moins six caractères et une combinaison de lettres, de chiffres et de symboles.
------------------	--

**Saisir le mot de passe de nouveau**

●●●●●●●●●●●●●●●●	Saisissez votre mot de passe de nouveau pour confirmer que vous n'avez pas fait d'erreur.
------------------	---

Figure 5: Les zones de texte du formulaire Mot de passe dûment remplies

Huitième étape. Cliquez sur  pour afficher la page du formulaire d'Entraide.

## 2.3 Le formulaire d'Entraide

En ce qui concerne l'aide financière et le bénévolat, **RiseUp** dépend entièrement de la générosité et de la gentillesse d'étrangers. Bien que leur demande de soutien financier soit tout à fait légitime et nécessaire, **RiseUp** encourage les utilisateurs à investir leur argent dans des projets locaux en faveur de la justice sociale. Il n'en tient qu'à vous de décider si vous ou votre organisme êtes en mesure d'offrir une contribution financière.

**Commentaire:** Votre décision n'affectera en rien le processus d'enregistrement de votre compte. Vous pourrez continuer à créer votre compte **RiseUp** gratuitement.

## fr, mutual\_aid

Ce service n'est pas gratuit. Il faut beaucoup de temps et d'argent pour maintenir riseup.net en vie. Dans un contexte où la surveillance est omniprésente et la publicité ciblée, nous croyons qu'il est plus important que jamais que les mouvements de libération soient en mesure de maîtriser leur propres moyens de communication. Veuillez contribuer, dans la mesure de vos moyens, à faire en sorte que nos serveurs fonctionnent et que nous puissions développer nos services. Vous ne recevrez pas un meilleur service si vous faites un don, mais votre karma vous remerciera. Pour des raisons de sécurité, nous n'enregistrons pas les dons. Cependant, nous vous enverrons des aide-mémoire selon la configuration que vous spécifiez ici.

### Fréquence du don

jamais	À quelle fréquence souhaitez-vous faire un don?
--------	---

### Montant du don

0.0	Combien? Si vous vivez dans le Sud ou dans un contexte défavorisé, veuillez contribuer à des projets locaux plutôt qu'à Riseup.net. Merci.
-----	--

<< Précédent   Suivant >>

Figure 6: Le formulaire fr, Entraide

Neuvième étape. Cliquez sur  pour afficher le formulaire *Activation*.

## 2.4 Le formulaire d'Activation

C'est dans le formulaire *Activation* que vous êtes invité à saisir vos codes d'activation.

Dixième étape. Saisissez les deux *codes d'invitation* dans les zones de texte appropriées.

### Activation

Il existe deux moyens de faire approuver la création de votre compte: vous devez soit recevoir des codes d'invitation de la part d'utilisateurs existants, soit attendre que nous approuvions votre requête. Si vous utilisez la méthode par invitation, chaque code doit provenir d'un utilisateur différent.

#### Codes d'invitation

First	opnegahg
Second	ohapieng

Figure 7: Un exemple de formulaire d'Activation dûment rempli

Onzième étape. Cliquez sur  pour conclure le processus de création de votre compte **RiseUp**:



Votre compte a été créé et vous pouvez l'utiliser dès maintenant. Visitez mail.riseup.net pour utiliser votre nouveau compte. Pour obtenir de l'aide, rendez vous à help.riseup.net.

Figure 8: Un exemple de confirmation de création du compte

Douzième étape. Cliquez sur  pour revenir à la *figure 2*.

Félicitations! Vous avez réussi à créer un compte de courriel **RiseUp** et vous serez automatiquement redirigé vers la *Figure 2*.

## Comment vous connecter à votre compte Riseup

Sommaire des sections de cette page:

- [3.0 Comment vous connecter à votre compte RiseUp](#)
- [3.1 Comment utiliser le Virtual Keyboard](#)

### 3.0 Comment vous connecter à votre compte RiseUp

Pour vous connecter à votre compte **RiseUp**, suivez les étapes énumérées ci-dessous:

**Première étape.** Ouvrez la page d'accueil de **RiseUp** eMail en mode SSL <https://mail.riseup.net/> <sup>[131]</sup>

Your connection is encrypted.  
If you want your email to be secure,  
please [read more on email security](#).

Webmail Server:

**Squirrel Webmail**  
Check your mail using [SquirrelMail 1.4.13](#)  
User:   
Password:   
  
Are you using a public computer? Enter your password with the [virtual keyboard](#).

**IMP Webmail**  
Check your mail using [IMP 4.1.6](#)  
User:   
Password:   
Language:

Figure 1: La page de connexion de RiseUp Mail

La page de connexion au service de courriel de **RiseUp** est séparée en deux, avec la section de *connexion* à gauche et les *Nouvelles* à droite.

**Commentaire:** Vous avez le choix entre deux systèmes de *webmail*. Vous pouvez utiliser l'un ou l'autre des système *webmail*, mais le *\*webmail IMP* est mieux adapté aux interfaces qui ne sont pas en anglais.

**Deuxième étape.** Saisissez l'information appropriée dans les zones de texte *User* et *Password*, soit dans la section *Squirrelmail*, soit dans la section *IMP webmail*. N'incluez pas la formule '@riseup.net' dans la zone de texte *User*.

**Étape optionnelle.** Sélectionnez votre langue d'usage dans le menu défilant *Language*, dans la section *IMP webmail*, si nécessaire.

**Troisième étape.** Cliquez sur  pour afficher votre compte:

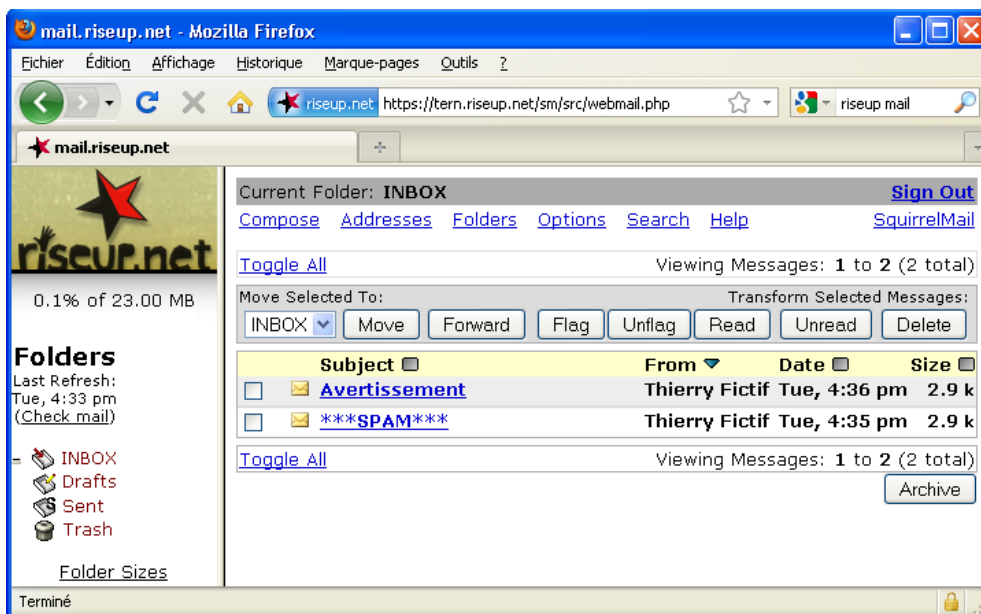


Figure 2: Un exemple de compte de courriel électronique RiseUp

**Étape optionnelle:** Si vous écrivez et recevez surtout des courriels dans une police de caractères non latine, vous voudrez sans doute le spécifier dans votre compte *webmail*. Sélectionnez [Options](#) dans le menu du haut pour afficher les options de *SquirrelMail*:

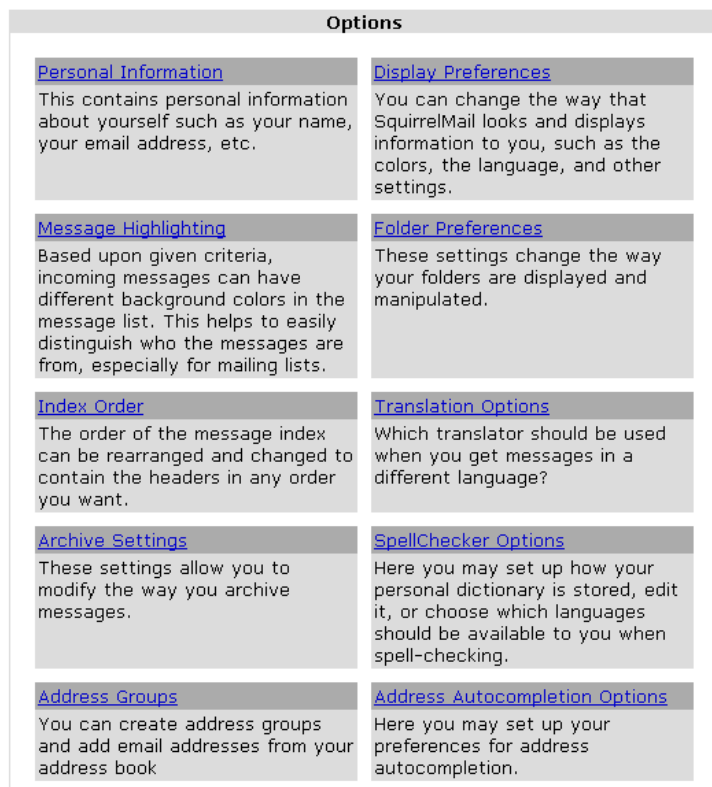


Figure 3: Les options de SquirrelMail

**Quatrième étape.** Sélectionnez [Display Preferences](#) pour afficher le panneau *Options - Préférences d'affichage*, illustré ci-dessous:

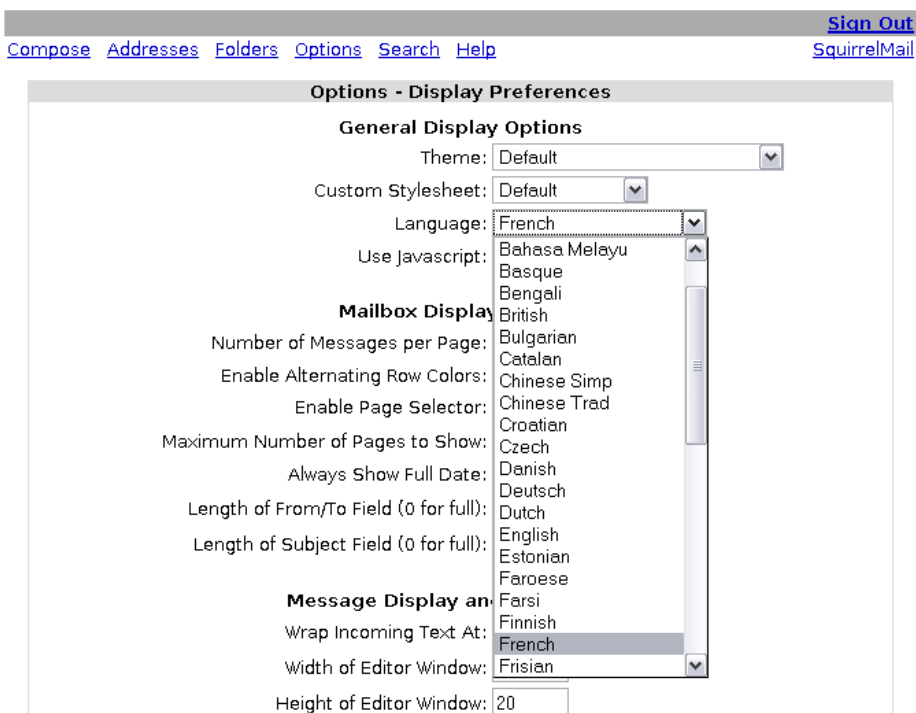


Figure 4: Le panneau *Options - Préférences d'affichage* de SquirrelMail

**Cinquième étape.** Trouvez le menu défilant *Language*, illustré à la figure 4 ci-dessus, puis sélectionnez la langue appropriée, dans cet exemple, *Français*.

Cette option servira à déterminer l'encodage approprié à l'affichage des messages que vous enverrez et recevrez.

### 3.1 Comment utiliser le Clavier virtuel

Si vous utilisez un ordinateur public ou partagé (dans un café Internet, un centre communautaire ou une bibliothèque, par exemple), vous pouvez utiliser le *Clavier virtuel (Virtual Keyboard)* pour saisir votre mot de passe. Cette méthode vous offre une mesure de protection supplémentaire contre les *enregistreurs de frappe* (programmes *key-logger*). Les enregistreurs de frappe sont conçus pour contrôler les séquences de frappe d'un utilisateur sur un clavier physique et ainsi

déduire les mots de passe, les noms d'utilisateur et autres renseignements importants. Les claviers virtuels contournent cette vulnérabilité en permettant aux utilisateurs de saisir un mot de passe à l'aide d'une souris.

Pour utiliser le *Clavier virtuel* de **RiseUp**, suivez les étapes énumérées ci-dessous:

**Première étape.** Ouvrez la page d'accueil de **RiseUp** en mode SSL <https://mail.riseup.net/> <sup>[131]</sup>.

**Deuxième étape.** Cliquez sur [virtual keyboard](#) pour afficher la page de connexion de **RiseUp**, tel qu'illustré ci-dessous:



Are you using a public computer?  
Enter your password with the [virtual keyboard](#)

Figure 5: La page de connexion de RiseUp

**Troisième étape.** Cliquez sur [virtual keyboard](#) pour afficher le *Clavier virtuel*, tel qu'illustré ci-dessous:

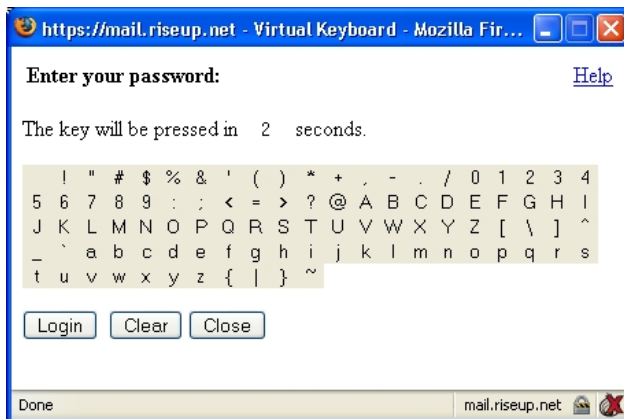


Figure 6: Le Clavier virtuel

**Quatrième étape.** À l'aide de votre souris, **cliquez** sur sur les touches qui forment votre mot de passe (ou positionnez votre curseur au dessus de chaque caractère pendant deux secondes).

**Cinquième étape.** Cliquez sur [Log in](#) pour accéder à votre compte **RiseUp**.

## Comment modifier les paramètres de votre compte

Sommaire des sections de cette page:

- [4.0 Comment modifier les paramètres de votre compte](#)
- [4.1 La page Mes paramètres](#)
- [4.2 La page des paramètres du Courriel](#)
- [4.3 La page Invitations](#)

---

### 4.0 Comment modifier les paramètres de votre compte

**RiseUp** vous permet de modifier certains paramètres de votre compte. Vous pouvez préciser la taille de votre boîte aux lettres, changer votre nom d'utilisateur, votre adresse et votre mot de passe, ajouter des alias, etc. Vous pouvez également générer des codes d'invitation pour aider vos amis et collègues à enregistrer leur propre compte **RiseUp**.


**Première étape.** Ouvrez la page de configuration de l'utilisateur **RiseUp Account Settings**: <https://user.riseup.net/> <sup>[132]</sup>

français

Nom d'utilisateur  
  
Mot de passe  
  
  
[J'ai oublié mon mot de passe](#)

## user.riseup.net

Bienvenue au panneau de configuration de l'utilisateur riseup.net. D'ici, vous pourrez gérer les paramètres de votre compte, tel que votre mot de passe, votre nom de domaine, votre quota et vos alias. Cette interface est actuellement en construction et offrira bientôt d'autres fonctions utiles.

 Nest where Riseup birds call home, it is where you can edit all of your your settings.

[Request a new account](#)  
[Créer un billet de dépannage](#)

Figure 1: La page user.riseup.net

**Deuxième étape.** Saisissez vos détails de connexion dans les zones de texte *Nom d'utilisateur* et *Mot de passe*.

**Troisième étape.** Cliquez sur  pour afficher la fenêtre suivante:

riseup.net home mail lists hosting help status donate

thierryfictif  
Panneau de configuration de l'utilisateur %s

français

- Mes paramètres
- Courriel
- Billets de dépannage
- Mutual Aid
- Invites
- Shell
- Logout

### Page d'accueil de %s

Bienvenue au panneau de configuration de votre compte d'utilisateur. Bientôt, ce sera pour vous un endroit important où vous pourrez régler vos préférences, obtenir de l'aide et demander de nouveaux services. Actuellement, le panneau de configuration permet uniquement le réglage des préférences du compte de courriel.

#### Obtenir de l'aide

- [M'aider avec mon compte de courriel »](#)
- [M'aider avec mon liste de diffusion »](#)


#### Demander un nouveau service

- [Close my email account »](#)
- More to come soon...

Figure 2: La page de configuration du compte d'utilisateur RiseUp.net

### 4.1 La page Mes paramètres

La page *Mes paramètres* affiche tous les renseignements que vous avez consignés à votre compte à la section **2.1 Le formulaire d'Information sur le compte** <sup>[133]</sup>.

**Première étape.** Cliquez sur  pour afficher la fenêtre suivante:

Mes paramètres

Courriel

Billets de dépannage

Mutual Aid

Invites

Shell

Logout

## Paramètres pour %s

Sur cette page, vous pouvez régler vos paramètres géxC3

### À propos de moi

#### Nom d'utilisateur

thierryfictif Pour modifier votre adresse de courriel principale, saisissez un nouveau nom d'utilisateur ici. Si vous préférez, vous pouvez choisir plutôt d'ajouter des alias à votre compte.

#### Adresse de courriel de rechange

Si vous indiquez une ou plusieurs adresses de courriel de rechange, nous les utiliserons pour communiquer avec vous lorsqu'il sera impossible de le faire via votre compte riseup.net. Si vous oubliez votre mot de passe, il vous sera possible d'en recevoir un nouveau à l'une de ces adresses. Si vous indiquez plus qu'une adresse, veuillez les séparer l'une de l'autre par une espace.

#### Afficher le nom

Thierry Fictif C'est le nom qui sera affiché lorsque vous créez ou répondez à des billets d'aide.

### Mot de passe

#### Question secrète

Quelle est ta couleur préférée? Si vous oubliez votre mot de passe, il vous sera possible de le changer en répondant à cette question de mot de passe. C'est pourquoi il est important que vous choisissiez une question dont vous seul connaissez la réponse.

#### Réponse secrète

coqe7ty08e7t3g Ceci est la réponse secrète à votre question de mot de passe.

#### Anniversaire

Avant de pouvoir changer votre mot de passe en répondant à votre question secrète, vous devrez indiquer votre date d'anniversaire, telle que vous l'aurez saisie ici.

#### Mot de passe

Si vous souhaitez changer de mot de passe, saisissez votre nouveau mot de passe ici.

#### Saisir le mot de passe de nouveau

Saisissez votre mot de passe de nouveau pour vérifier que vous n'avez pas fait d'erreur.

### Région

#### Langue

français Ce paramètre détermine la langue choisie par défaut lorsque vous utilisez le panneau de configuration de l'utilisateur.

#### Pays

Nous utilisons l'information sur le pays pour déterminer les langues d'usage et les emplacements de nos prochains serveurs. Ces renseignements sont optionnels.

#### Fuseau horaire

Tous les affichages de l'heure seront réglés selon ce fuseau horaire.

Sauvegarder les changements

Figure 3: La page Mes paramètres

Dans cette fenêtre, vous pouvez changer de nom d'utilisateur, ce qui modifiera également votre adresse de courrier électronique. Le nouveau nom d'utilisateur doit donc être original. C'est aussi sur cette page qu'il vous est possible de modifier d'autres paramètres du compte, tel que votre adresse de courriel de rechange, votre mot de passe, et ainsi de suite.

**Première étape.** Saisissez les nouveaux renseignements dans les zones appropriées, puis cliquez sur **Sauvegarder les changements** pour afficher le message suivant:



Les changements ont été sauvegardés.

Figure 4: Changements sauvegardés avec succès

## 4.2 La page des paramètres du Courriel

La page *paramètres du Courriel* vous permet d'afficher ou de modifier les paramètres de stockage de votre courrier électronique. Vous pouvez déterminer le "quota" ou l'espace réservé à votre compte webmail sur un des serveurs de **RiseUp**.



Courriel

**Première étape.** Cliquez sur pour afficher la fenêtre suivante:



 [Mes paramètres](#)

 **Courriel**

 [Billets de dépannage](#)

 [Mutual Aid](#)

 [Invites](#)

 [Shell](#)

 [Logout](#)

## Email paramètres

[Ma boîte de courriel](#)

[Paramètre de gestion des pourriels](#)

[filtres-courriel](#)

Sur cette page, vous pouvez régler vos préférences de messagerie, tel que vos quotas, vos alias et vos transferts de messages.

<b>Adresse</b>	thierryfictif@riseup.net	Voici votre adresse de courriel. Pour toute modification, rendez vous à "Mes paramètres".
<b>Conserver les fichiers de sauvegarde</b>	<input checked="" type="checkbox"/>	Si vous cochez cette option, nous conserverons une copie de sauvegarde de vos courriels. Si nos serveurs explosent ou si votre client de messagerie supprime tous vos courriels, vous serez en mesure de récupérer toutes vos donxC3
<b>Quota</b>	23 mégaoctets	Vous pouvez régler vous-même le quota de votre boîte de courriel. Cependant, n'oubliez pas que l'espace de stockage constitue notre dépense matérielle la plus importante. Si vous augmentez votre quota, veuillez également augmenter votre contribution !
<b>Hôte du stockage</b>	cormorant-pn.riseup.net	Ceci est le nom d'hôte Internet du serveur où vos courriels sont stockés. Veuillez éviter de faire pointer votre client IMAP ou POP directement vers votre hôte Internet.

### Alias et transferts

<b>Alias</b>	tresbontesteur testeursur	Les alias sont des adresses de courriel supplémentaires que votre compte peut utiliser pour recevoir des courriels. Indiquez une adresse de courriel complète, à raison d'une par ligne. Pour l'instant, seulement les adresses @riseup.net sont permises.
<b>Transférer</b>	<input type="text"/>	Indiquez une adresse de courriel où seront transférés tous les courriels expédiés à votre compte riseup.net. Tant et aussi longtemps que vous aurez un transfert configuré, vous ne recevrez aucun courriel à riseup.net.

[Réparer la boîte de courriel](#) | [Restore mail from backups](#) | [Détruire la boîte de courriel](#)

[Sauvegarder les changements](#)

Figure 5: La page des paramètres du Courriel

**Deuxième étape.** Saisissez un nombre approprié dans la zone *Quota*.

**Commentaire:** La taille de votre compte est limitée à un maximum de 47 Mo. Cela est considéré comme une taille suffisante pour les communications par courriel.

**RiseUp** n'est peut-être pas le meilleur choix si vous souhaitez utiliser un compte de courriel pour envoyer et recevoir plusieurs pièces jointes de grande taille.

Vous pouvez également créer des alias pour votre compte. Un alias est comme un surnom pour votre compte. Alors que le nom de compte principal restera inchangé, on pourra également envoyer des messages aux adresses de vos alias.

#### Alias et transferts

<b>Alias</b>	tresbontesteur testeursur	Les alias sont des adresses de courriel supplémentaires que votre compte peut utiliser pour recevoir des courriels. Indiquez une adresse de courriel complète, à raison d'une par ligne. Pour l'instant, seulement les adresses @riseup.net sont permises.
--------------	------------------------------	--

Figure 6: La section Alias

**Exemple:** Le compte **thierryfictif@riseup.net** comporte maintenant deux alias. Les messages expédiés à **tresbontesteur@riseup.net** et à **testeursur@riseup.net** seront transférés au compte principal. Cela peut s'avérer pratique pour garder votre véritable adresse confidentielle.

**Quatrième étape.** Cliquez sur  pour sauvegarder vos nouveaux alias.

## 4.3 La page Invitations

La page *Invitations* vous permet de générer des *codes d'invitation* qui servent à inviter vos amis et collègues à créer un compte **RiseUp**.

**Important:** Rappelez-vous que chaque nouveau compte exige deux codes d'invitation provenant de deux membres différents. Vous pouvez générer autant de codes que vous le souhaitez.

 [Invitations](#)

**Première étape.** Cliquez sur  pour afficher la fenêtre suivante:



Figure 7: La page Invitations

**Deuxième étape.** Cliquez sur  pour générer des codes d'invitation:

Code	Expire le
uzamaloo	Feb 25 2011
niejuhai	Feb 25 2011

Figure 8: Un exemple de code d'invitation généré automatiquement

**Commentaire:** Chaque code d'invitation n'est valide que pour un mois.

**Troisième étape.** Cliquez sur  pour imprimer une copie des codes d'invitation et la remettre à la personne qui souhaite

enregistrer un compte avec **RiseUp**.



**Quatrième étape.** Cliquez sur  pour vous déconnecter de l'interface *Utilisateur*.

## Faq et questions récapitulatives

### 5.0 Faq et questions récapitulatives

Muhindo et Salima sont ravis de constater à quel point il est facile d'utiliser **RiseUp** et sont impressionnés par l'engagement du collectif envers des valeurs sociales progressistes. Par contre, quelques questions subsistent. Heureusement leur père, Assani, est en mesure de leur donner les réponses.

**Q:** Dans quelles circonstances devrait-on utiliser **IMP** plutôt que **SquirrelMail**?

**A:** Bonne question! En fait, il n'y a pas vraiment de différence. Si, pour une raison ou une autre, un des service webmail ne fonctionne pas ou est en cours de réparation ou de mise à jour, vous pouvez toujours utiliser l'autre service sans interruption. De plus, **IMP** offre un meilleur service pour les utilisateurs non anglophones.

**Q:** En créant mon compte, j'ai réalisé que je ne suis pas obligé de fournir des renseignements privés.

**A:** En effet, personne n'est obligé de le faire. Par contre, n'oubliez pas de changer vos mots de passe tous les 3 à 6 mois.

**\*Q:** Maintenant que Muhindo et moi disposons de comptes **RiseUp**, comment pouvons-nous en enregistrer un pour toi Assani? \*

**A:** Vous devez tous les deux créer un code d'invitation, puis me les envoyer. Lorsque je créerai mon propre compte, j'utiliserai vos codes d'invitation.

**Commentaire:** Comme **RiseUp** dépend entièrement de dons et de la bonne volonté et du travail acharné d'une équipe de bénévoles, il n'est pas facile de faire compétition aux fournisseurs commerciaux de services de courrier électronique. Néanmoins, **RiseUp** a mis en ligne sa propre alternative (gratuite et en source ouverte) à **Facebook**, nommée **Crabgrass**. Le service présente des normes de confidentialité et de sécurité accrues et s'adresse principalement aux organismes communautaires et aux organisations non gouvernementales, ainsi qu'aux organismes de base. Pleine d'ambition et d'énergie, l'équipe de **RiseUp** espère être en mesure d'offrir ces services compétitifs et révolutionnaires dans un avenir rapproché:

- Édition collective de documents (**Etherpad**): Ce service permet à plusieurs utilisateurs d'éditer simultanément un même document.
- Proxy Internet chiffré (**openvpn**): Ce service permet de naviguer sur Internet en utilisant un serveur proxy chiffré semblable à **Tor**.
- Clavardage en temps réel (**XMPP**): Ce service permet de clavarder en temps réel et constitue l'équivalent **RiseUp** de la fonction *chat* de **Gmail** ou de la **Messagerie instantanée de Microsoft**.

### 5.1 Questions récapitulatives

- Quelle est la différence entre la récupération du courriel par Webmail ou à l'aide d'un client de messagerie?
- Qu'est-ce qu'un *Secure Socket Layer (SSL)* et comment cela fonctionne t-il?
- Qu'est-ce qu'un clavier virtuel, et comment cela fonctionne t-il?
- Comment peut-on ajouter un alias à un compte de courriel?
- Combien de temps un code d'invitation demeure t-il valide?

## Pidgin + OTR - messagerie instantanée sécurisée

**Short Description:**

Pidgin est un client gratuit et de source ouverte qui vous permet d'organiser et de gérer vos différents comptes de **messagerie instantanée (MI)** à l'aide d'une seule et unique interface. Le module complémentaire **Off-the-Record (OTR)** est conçu spécialement pour être utilisé avec **Pidgin** pour sécuriser et authentifier les communications entre utilisateurs de **Pidgin**.

**Online Installation Instructions:**

**Pour installer Pidgin et OTR**

- Lisez la courte introduction des **Guides pratiques** <sup>[1]</sup>.
- Cliquez sur l'icône de **Pidgin** ci-dessous pour ouvrir la page <http://www.pidgin.im/download/windows/>.
- Cliquez sur le lien **Download Pidgin for Windows**.
- Sauvegardez le fichier d'installation, puis **trouvez-le** et **double-cliquez** dessus.
- Cliquez sur l'icône **OTR** ci-dessous pour ouvrir la page [www.cypherpunks.ca/otr](http://www.cypherpunks.ca/otr).
- Cliquez sur le lien **Win32 installer for pidgin** dans la section **OTR plugin for Pidgin**.
- Sauvegardez le fichier d'installation, puis **trouvez-le** et **double-cliquez** dessus.
- Après avoir complété l'installation de **Pidgin** et **OTR**, vous pouvez supprimer les fichiers d'installation.

Pidgin: OTR:



Off-the-Record <sup>[135]</sup>

<sup>[134]</sup>

<sup>[135]</sup>

Site Internet

- Pidgin: [www.pidgin.im](http://www.pidgin.im) <sup>[136]</sup>
- OTR: [www.cypherpunks.ca/otr](http://www.cypherpunks.ca/otr) <sup>[137]</sup>

Configuration requise:

- Une connexion Internet
- Compatible avec toutes les versions de Windows

Versions utilisées pour rédiger ce guide:

- Pidgin 2.10.3
- OTR 3.2.0

Licence:

- FLOSS (Free/libre Open Source Software)

Lecture requise:

Livret pratique Security in-a-box, chapitre **7. Préserver la confidentialité de vos communications sur Internet** <sup>[126]</sup>

Niveau: 1: Débutant, 2: Moyen, 3: Intermédiaire, 4: Expérimenté, 5: Avancé

Temps d'apprentissage: 30 minutes

\*\*Ce que vous apportera l'utilisation de cet outil \*\*:

- La capacité d'organiser et de gérer certains des services de messagerie instantanée les plus connus à l'aide d'un seul programme;
- La possibilité de mener des séances de clavardage (chat) privées et sécurisées.

Autres programmes compatibles avec GNU Linux, Mac OS ou Microsoft Windows:

**Pidgin** et **OTR** offrent des versions compatibles avec **Microsoft Windows** et **GNU/Linux**. **Miranda IM** <sup>[138]</sup> est un autre programme de **messagerie instantanée** multi-protocoles conçu **Microsoft Windows** et compatible avec **OTR**. Pour **Mac OS**, nous recommandons **Adium** <sup>[139]</sup>, un programme de **messagerie instantanée** multi-protocoles qui supporte le plugin **OTR**.

## 1.1 À propos de cet outil

**Pidgin** est un client de **messagerie instantanée (MI)** gratuit et de source ouverte qui vous permet d'organiser et de gérer vos différents comptes de **messagerie instantanée** avec une seule et unique interface. Avant de commencer à utiliser **Pidgin**, vous devez disposer d'au moins un compte de **MI**. Par exemple, si vous possédez un compte de courriel **Gmail**, vous pouvez utiliser le service de **MI Google Talk** avec **Pidgin**. Utilisez les détails de connexion associés à votre compte de **MI** pour y accéder via **Pidgin**.

**Note:** Tous les utilisateurs sont fortement encouragés à en apprendre le plus possible sur les politiques de leurs fournisseurs de service de **MI** en matière de confidentialité et de sécurité.

**Pidgin** est compatible avec les services de **MI** suivants: **AIM** <sup>[140]</sup>, **Bonjour** <sup>[141]</sup>, **Gadu-Gadu** <sup>[142]</sup>, **Google Talk** <sup>[143]</sup>, **Groupwise**, **ICQ** <sup>[144]</sup>, **IRC**, **MIRC** <sup>[145]</sup>, **MSN** <sup>[146]</sup>, **MXit** <sup>[147]</sup>, **MySpaceIM** <sup>[148]</sup>, **QQ** <sup>[149]</sup>, **SILC** <sup>[150]</sup>, **SIMPLE**, **Sametime** <sup>[151]</sup>, **Yahoo!** <sup>[152]</sup>, **Zephyr** ainsi que tous les clients de **MI** utilisant le protocole de messagerie **XMPP**.

**Pidgin** ne permet pas la communication entre différents services de **MI**. Par exemple, si vous utilisez **Pidgin** pour accéder à votre compte **Google Talk**, il ne vous sera pas possible de clavarder avec un ami qui utilise plutôt un compte **ICQ**.

Par contre, **Pidgin** peut être réglé pour gérer plusieurs comptes compatibles avec l'un ou l'autre des protocoles supportés. Autrement dit, vous pouvez simultanément utiliser un compte **Gmail** un compte **ICQ**, et clavarder avec des correspondants qui utilisent l'un ou l'autre de ces services (qui sont supportés par **Pidgin**).

Il est conseillé d'utiliser **Pidgin** pour tous vos besoins en matière de **messagerie instantanée**, puisque ce programme offre plus de sécurité que la plupart des options qui existent et ne vient pas par défaut avec des logiciels publicitaires ou espions superflus qui pourraient compromettre votre sécurité ou votre vie privée.

La messagerie **Off-the-Record (OTR)** est un module complémentaire, conçu tout spécialement pour **Pidgin**, qui permet de clavarder en privé et offre les fonctions suivantes:

- **Authentification:** Vous êtes assuré que votre correspondant est bel et bien la personne que vous croyez.
- **Possibilité de démenti (deniability):** Après votre conversation, il est impossible de retracer les messages jusqu'à vous ou jusqu'à votre correspondant.

- **Chiffrement:** Personne d'autre que vous ne peut lire vos communications instantanées.
- **Perfect Forward Secrecy:** Si une tierce partie trouve l'accès à vos clés privées, vos conversations préalables ne sont pas compromises.

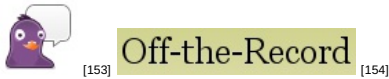
**Note:** Vous devez installer le programme **Pidgin** avant d'installer le plugin **OTR**.

#### Offline Installation Instructions :

#### Pour installer Pidgin + OTR

- \*Lisez la courte **Introduction** aux **Guides pratiques** <sup>[1]\*\*</sup>
- **Cliquez sur l'icône Pidgin + OTR ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.

**Pidgin: OTR:**



## Comment installer Pidgin et OTR, s'inscrire et régler votre compte pour fonctionner avec Pidgin

Sommaire des sections de cette page:

- [2.0 À propos de Pidgin](#)
- [2.1 Comment installer Pidgin](#)
- [2.2 Comment installer le moteur Off-The-Record \(OTR\)](#)
- [2.3 Un survol de la procédure d'enregistrement et de configuration de Pidgin](#)
- [2.4 Comment enregistrer votre compte de messagerie instantanée dans Pidgin](#)
- [2.5 Comment ajouter un contact dans Pidgin](#)
- [2.6 Comment votre correspondant Pidgin peut vous ajouter comme Contact](#)
- [2.7 Comment ouvrir une fenêtre de MI dans Pidgin](#)
- [2.8 Comment réactiver un compte dans Pidgin](#)

## 2.0 À propos de Pidgin

**Pidgin** et le moteur de chiffrement et d'authentification **Off-the-Record (OTR)** doivent être installés correctement pour fonctionner normalement. Heureusement la procédure d'installation des deux programmes est simple et rapide.

## 2.1 Comment installer Pidgin



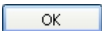
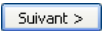
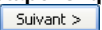
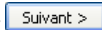
**Première étape.** Double-cliquez sur  pidgin-2.10.3 ; si une fenêtre *Fichier ouvert - Avertissement de sécurité* s'ouvre, cliquez sur  pour afficher la fenêtre suivante:

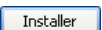


Figure 1: La fenêtre de sélection de la langue d'installation

**Deuxième étape.** Cliquez sur  pour afficher la fenêtre du *Programme d'installation de Pidgin 2.10.3*.

**Troisième étape.** Cliquez sur  pour afficher la fenêtre *Licence utilisateur*; après avoir lu la *Licence d'utilisation*, cliquez sur  pour afficher la fenêtre *Installation de Pidgin 2.10.3 - Choisissez les composants*.

**Quatrième étape.** Cliquez sur  pour afficher la fenêtre *Installation de Pidgin 2.10.3 - Choisissez le dossier d'installation*.

**Cinquième étape.** Cliquez sur  pour accepter le dossier d'installation par défaut, afficher la fenêtre *Installation de Pidgin 2.10.3 - Installation en cours* et lancer l'installation du logiciel **Pidgin**.

Un certain nombre de répertoires et de fichiers s'installent alors en rafale; lorsque la procédure d'installation est terminée, la fenêtre *Installation de Pidgin 2.10.3 - Fin de l'installation* s'affiche.

**Sixième étape.** Cliquez sur  pour afficher la fenêtre *Fin de l'installation*.


L'étape suivante est facultative:

**Septième étape.** Cochez l'option  Lancer Pidgin 2.10.3 si vous souhaitez lancer **Pidgin** immédiatement.

**N. B.:** À la troisième étape de la procédure d'installation, **Pidgin** a été configuré pour ajouter un lien au menu **Démarrer > Programmes**, et peut être lancé à partir de cette liste à l'avenir.

Huitième étape. Cliquez sur  pour finaliser la procédure d'installation de **Pidgin**.

## 2.2 Comment installer le moteur Off-The-Record (OTR)

Première étape. Double-cliquez sur  `pidgin-otr-3.2.0-1.exe`; si une fenêtre *Fichier ouvert - Avertissement de sécurité* s'ouvre, cliquez sur  pour afficher la fenêtre suivante:

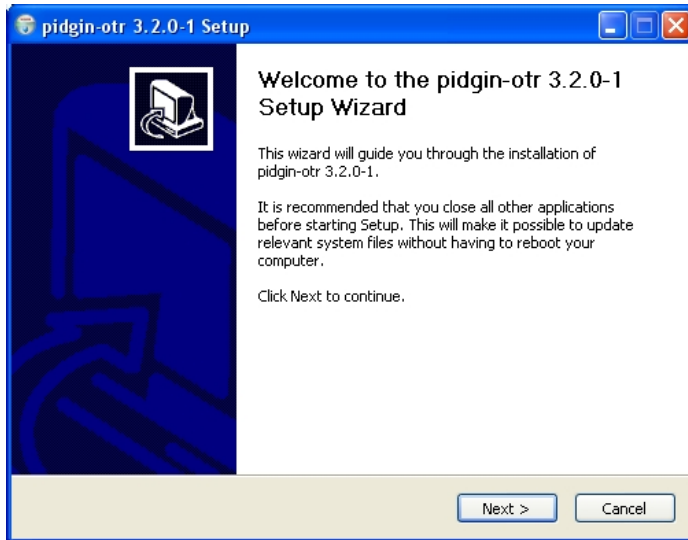


Figure 2: La fenêtre *Welcome to the pidgin-otr 3.2.0-1 Setup Wizard*

Deuxième étape. Cliquez sur  pour afficher la fenêtre *License Agreement*; après avoir lu la *Licence d'utilisation*, cliquez sur  pour afficher la fenêtre *pidgin-otr 3.2.0-1 Setup - Choose Install Location*.

Troisième étape. Cliquez sur  pour lancer la procédure d'installation.

Quatrième étape. Cliquez sur  pour finaliser l'installation du moteur **Pidgin-OTR**.

Lorsque vous avez complété l'installation de **Pidgin** et **OTR**, l'icone suivant apparaît dans la barre des tâches de Windows:



Figure 3: L'icone *Pidgin-OTR* dans la barre des tâches

Félicitations! Vous avez complété l'installation des programmes **Pidgin** et **OTR**!

## 2.3 Un survol de la procédure d'enregistrement et de configuration de Pidgin

Il y a quatre étapes de base à suivre pour enregistrer et régler **Pidgin**: enregistrer un compte de **MI** existant dans **Pidgin**; ajouter un correspondant, ou *contact* dans le vocabulaire de **Pidgin**; demander à votre contact de faire la même chose; et finalement, accéder à la fenêtre de clavardage pour entamer votre première séance de *chat*.

Puisque une séance de *messaging instantané* a lieu entre deux parties, les exemples sur cette page décrivent comment les divers formulaires et fenêtres s'affichent pour les *deux* contacts/correspondants (représentés par deux personnages fictifs, Salima et Thierry) à différentes étapes de la procédure d'enregistrement et de configuration. Tous les exemples sont du protocole **Google Talk**.

**N. B.:** Avant de commencer à utiliser **Pidgin**, vous devez déjà disposer d'un compte de **messaging instantané (IM)** avec l'un des fournisseurs listés à la *Figure 3*. Si vous souhaitez créer un compte d'*IM*, nous recommandons fortement **Google Talk**. Veuillez vous référer à la section [4.0 Comment créer un compte Google Talk](#) <sup>[155]</sup> pour plus de renseignements.

## 2.4 Comment enregistrer votre compte de messaging instantané dans Pidgin

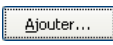
Pour enregistrer votre compte de **MI** dans **Pidgin**, veuillez suivre les étapes suivantes:



Première étape. Cliquez sur  ou sélectionnez **Démarrer > Pidgin** pour lancer **Pidgin**. À la première ouverture de **Pidgin**, la fenêtre suivante s'affiche:



Figure 4: La fenêtre de confirmation des comptes

Deuxième étape. Cliquez sur  pour afficher une fenêtre *Ajouter un compte* vierge, comme suit:

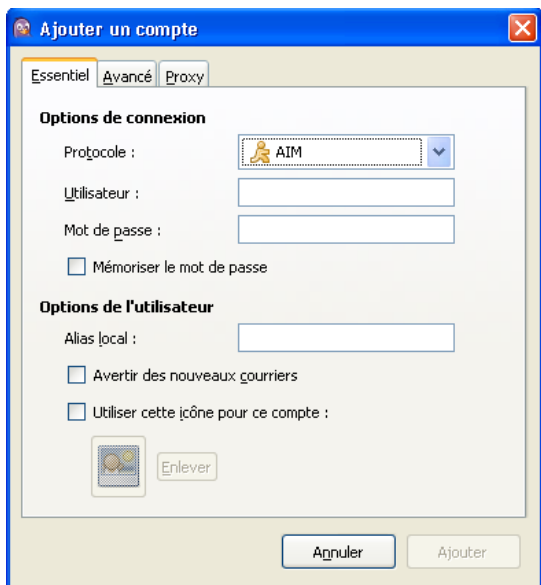


Figure 5: La fenêtre *Ajouter un compte* affichant les onglets *Essentiel*, *Avancé* et *Proxy*

Troisième étape. Cliquez sur le menu défilant *Protocole* pour visualiser les protocoles de service de **MI** supportés par **Pidgin**, tel qu'illustré ci-dessous:

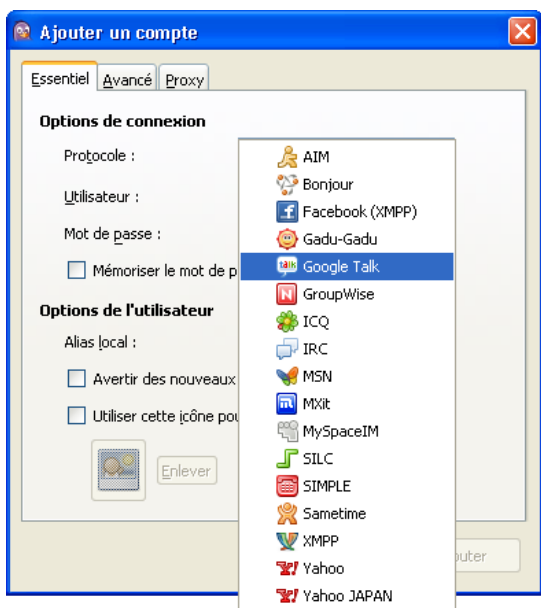


Figure 6: La fenêtre *Ajouter un compte* affichant la liste de protocoles de **MI** supportés

Quatrième étape. Sélectionnez le protocole de **MI** approprié.

**N. B. :** Certains fournisseurs de service de **MI** affichent leurs zones de texte particulières, que vous devez remplir. D'autres remplissent les zones de texte automatiquement (par exemple, si vous sélectionnez **Google Talk**, la zone de texte *Domaine* est déjà remplie pour vous). Cependant, tous les services exigent que vous saisissiez un nom d'utilisateur et un mot de passe.

**Cinquième étape.** Saisissez votre adresse de courrier électronique (par exemple, [thierry.letesteur@gmail.com](mailto:thierry.letesteur@gmail.com) <sup>[156]</sup>) dans la zone *Utilisateur*.

**Sixième étape.** Saisissez le mot de passe associé à ce compte dans la zone *Mot de passe*.

**Septième étape.** Saisissez un surnom par lequel vous souhaitez être identifié dans la zone *Alias local*. (Cette option est facultative.)

**Important:** Pour maximiser votre sécurité et votre confidentialité, il est souhaitable de laisser l'option *Mémoriser le mot de passe* décochée. Ainsi, **Pidgin** vous demandera de saisir votre mot de passe chaque fois que vous vous connecterez pour clavier. De cette manière, personne ne sera en mesure de se connecter en usurpant votre identité si vous vous éloignez de votre ordinateur pour une longue période. Aussi, n'oubliez jamais de quitter **Pidgin** en **sélectionnant** l'item *Quitter* lorsque vous avez fini une séance de clavardage!

Une fenêtre *Ajouter un compte* dûment remplie devrait ressembler à ceci :

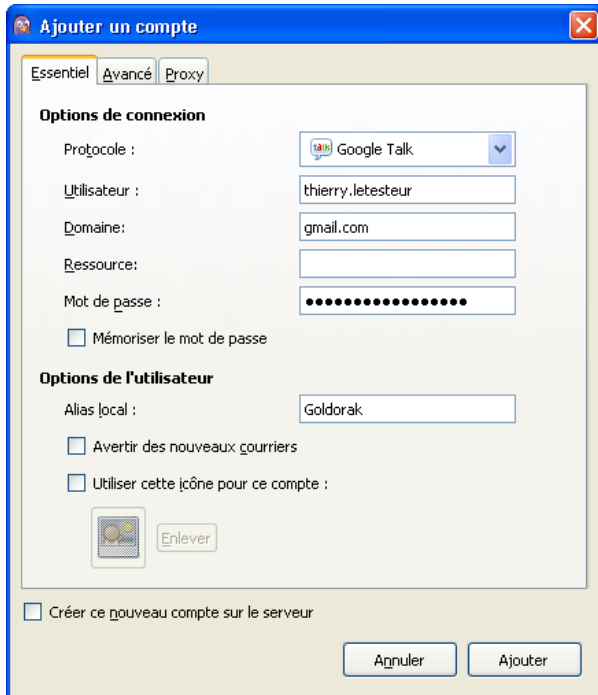


Figure 7: Exemple de formulaire *Ajouter un compte* dûment rempli

**Astuce:** Les clients **Google Talk**, **IRC**, **SILC** et **XMPP** sont facilement configurables pour exiger une connexion chiffrée. Veuillez pour cela consulter la section **5.1 Comment activer une connexion sécurisée** <sup>[157]</sup> pour plus de renseignements.

**Huitième étape.** Cliquez sur  pour finaliser la procédure d'ajout de compte et afficher la fenêtre *Comptes* et la *Liste de contacts*, telles qu'illustrées ci-dessous:

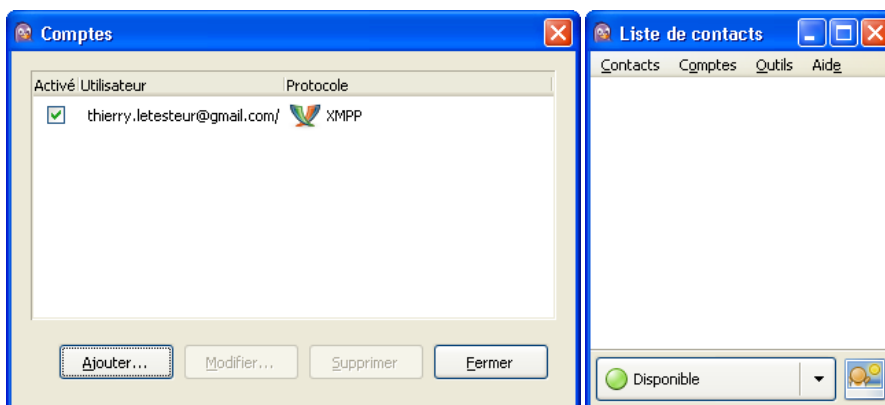


Figure 8: La fenêtre des *Comptes*; Figure 9: La liste de contacts en mode *Actif*

Après avoir complété ces étapes, vous êtes prêt à ajouter vos contacts **Pidgin** en saisissant leurs coordonnées respectives.

## 2.5 Comment ajouter un contact dans Pidgin

L'ajout de contacts, ou de correspondants, dans **Pidgin** implique que vous sauvegardiez leurs coordonnées. Dans l'exemple suivant, Thierry ajoute Salima à sa liste de contacts.

Pour ajouter un contact à votre compte de **IM** dans **Pidgin**, suivez les étapes énumérées ci-dessous:

**Première étape.** Cliquez sur *Contacts* pour afficher le menu correspondant, puis **sélectionnez** l'item *Ajouter un contact...*:





Figure 10: Le menu Contacts avec l'item "Ajouter un contact..." sélectionné

Cela affiche la fenêtre suivante:



Figure 11: La fenêtre ajouter le contact

**Deuxième étape.** Si vous avez plusieurs comptes, **sélectionnez** le compte qui correspond au service de messagerie instantanée employé par votre 'contact'.

**N. B.:** Il est *essentiel* que vous et votre contact utilisiez le *même* service de messagerie, et ce, même si cette personne n'utilise pas **Pidgin**. Par exemple, vous ne pourrez pas ajouter un contact **ICQ** ou **MSN** à un compte **Google Talk**. Par contre, vous pouvez enregistrer et utiliser simultanément plusieurs comptes dans **Pidgin**, ce qui vous permet de clavarder avec un contact via **Google Talk** et avec un autre via **ICQ** ou **MSN**.

**Troisième étape.** Saisissez l'adresse de courriel de votre contact dans la zone de texte *Nom d'utilisateur du contact*.

L'option suivante est facultative.

**Quatrième étape.** Saisissez un *Alias* ou un surnom pour votre contact dans la zone de texte *Alias (facultatif)*, de telle sorte que le formulaire *Ajouter le contact* ressemble à ceci:

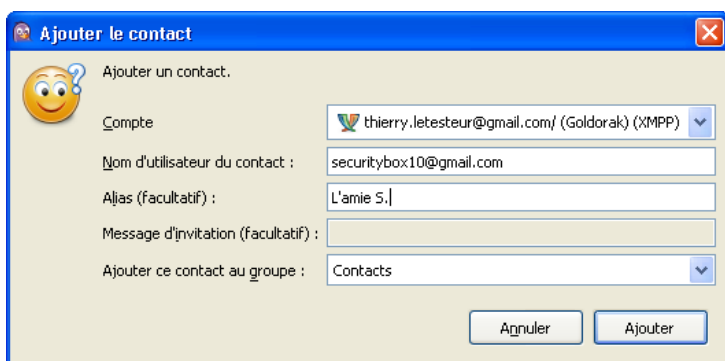


Figure 12: Un exemple de formulaire Ajouter le contact dûment rempli

**Cinquième étape.** Cliquez sur  pour ajouter votre contact.

**N. B.:** Après avoir ajouté un contact, un message sera envoyé automatiquement à ce dernier pour lui demander une approbation ou une autorisation, selon votre requête. Le message s'affichera ainsi dans sa *Liste de contacts*:

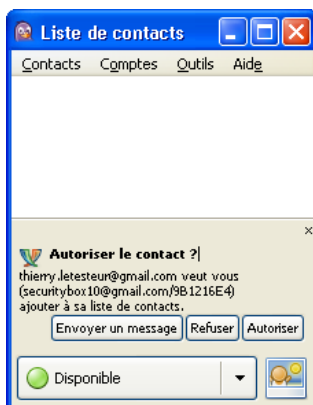


Figure 13: La demande d'autorisation d'un contact tel qu'affichée dans la liste de contacts de Salima

À ce stade, votre contact devrait suivre les étapes énumérées ci-dessous:

**Sixième étape.** Cliquez sur **Autoriser** pour ajouter cette personne en tant que contact et afficher son alias dans votre *Liste de contacts*, comme suit:

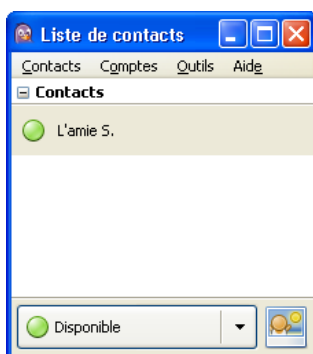


Figure 14: La liste de contacts de Thierry affichant Salima comme contact

**N. B.:** Dans l'exemple ci-dessus, c'est le surnom, ou l'*alias*, de Salima qui est affiché, ce qui ajoute un niveau supplémentaire de protection de l'identité.

## 2.6 Comment votre correspondant Pidgin peut vous ajouter comme Contact

Lorsque vous avez ajouté, autorisé et confirmé votre contact dans **Pidgin**, il ou elle doit suivre la même procédure avec vos propres coordonnées de **MI**.

Dans cette section, notre exemple montre comment Salima, à son tour, ajoute autorise et confirme Thierry comme contact dans **Pidgin**. Salima doit suivre les *étapes 1 à 6* de la section **2.5 Comment ajouter un contact dans Pidgin**.

Lorsque Salima a complété les *étapes 1 à 3*, sa fenêtre *Ajouter le contact* s'affiche comme suit:



Figure 15: La fenêtre "Ajouter le contact" de Salima

Salima doit ensuite **cliquer** sur **Ajouter** pour ajouter Thierry comme contact et lui envoyer en même temps la demande d'autorisation, comme suit:



Figure 16: La demande d'autorisation d'un contact telle qu'elle s'affiche dans le compte de Thierry

**N. B.:** Si vous placez votre curseur au-dessus d'un contact dans la *Liste des contacts*, un message s'affiche avec des coordonnées correspondantes:

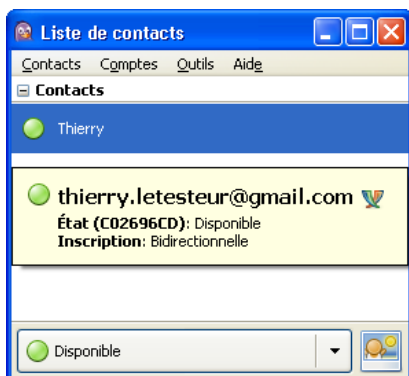


Figure 17: La liste de contacts de Salima affichant les coordonnées de Thierry

## 2.7 Comment ouvrir une fenêtre de MI dans Pidgin

Pour ouvrir une fenêtre de **MI** dans **Pidgin**, suivez les étapes énumérées ci-dessous:

**Première étape.** Cliquez à droite sur le nom de votre contact dans votre *Liste de contacts* pour afficher le menu de toutes les tâches que vous pouvez entreprendre, tel qu'illustré ci-dessous:

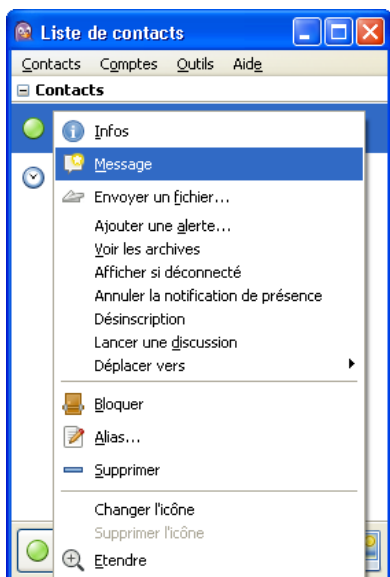


Figure 18: Le menu des tâches des contacts

**Deuxième étape.** Sélectionnez l'item *Message* dans le menu pour afficher une fenêtre de messagerie:

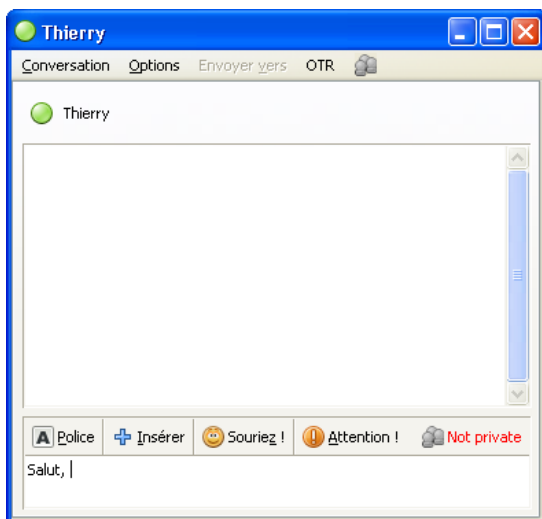


Figure 19: Une fenêtre de messagerie dans Pidgin

Vous êtes désormais fin prêt à clavarder avec votre contact en utilisant **Pidgin**. Cependant, il vous d'abord configurer **OTR** pour faire en sorte que vos séances de clavardage soient confidentielles et sécurisées.

## 2.8 Comment réactiver un compte dans Pidgin

Il arrive qu'un compte **Pidgin** soit désactivé, soit parce que votre connexion Internet a été interrompue, soit parce que votre ordinateur a subi une panne. Ces deux situations peuvent entraîner une interruption et une désactivation de votre compte **Pidgin**. Heureusement, **Pidgin** offre plusieurs possibilités pour réactiver votre compte.

Pour réactiver votre compte, suivez les étapes énumérées ci-dessous:



**Première étape.** Cliquez sur **Pidgin** ou sélectionnez **Démarrer > Pidgin** pour lancer **Pidgin**.

**Deuxième étape.** Ouvrez le menu **Comptes**, puis sélectionnez l'item **Gérer les comptes**:

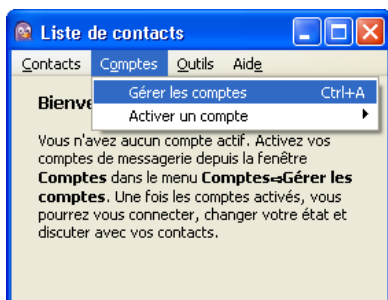


Figure 20: Le menu **Comptes** avec l'item **Gérer les comptes** sélectionné

La fenêtre suivante s'affiche alors:

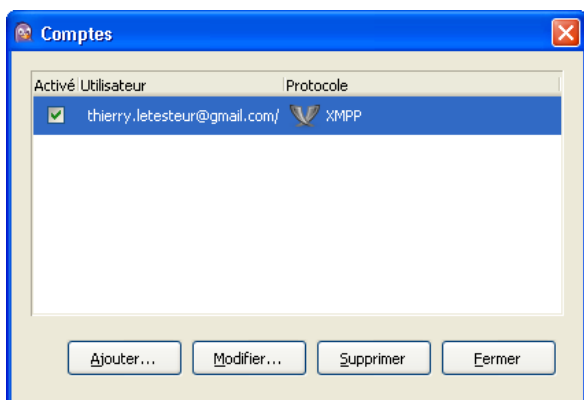


Figure 21: La fenêtre **Comptes** affichant le compte désactivé

**Troisième étape.** Cliquez sur la case à cocher adjacente au compte pour afficher la fenêtre de mot de passe de **Pidgin**:

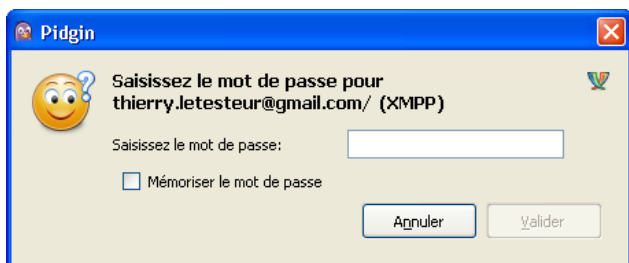


Figure 22: La fenêtre de mot de passe de Pidgin

**Quatrième étape.** Saisissez votre mot de passe **Pidgin**, de telle sorte que la fenêtre ressemble à ceci:

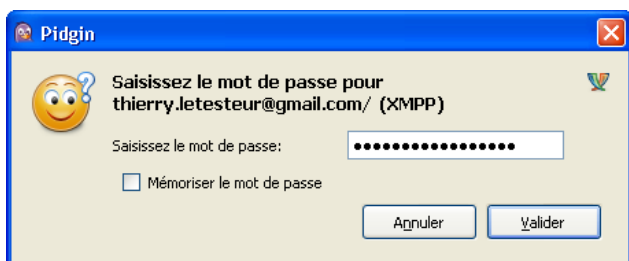


Figure 23: La fenêtre de mot de passe de Pidgin avec la zone de texte remplie

**Cinquième étape.** Cliquez sur  pour compléter la réactivation de votre compte:

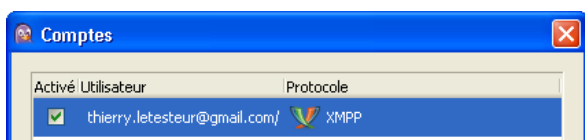


Figure 24: Un exemple de compte réactivé

**Sixième étape.** Cliquez sur  pour fermer la fenêtre *Comptes*.

## Comment sécuriser vos séances de clavardage avec OTR

Sommaire des sections de cette page:

- [3.0 À propos de Pidgin et d'OTR](#)
- [3.1 Comment configurer le plugin Pidgin-OTR](#)
- [3.2 La première étape - Comment produire une clé privée et afficher son empreinte](#)
- [3.3 La deuxième étape - Comment authentifier une séance de clavardage privée](#)
- [3.4 La troisième étape - Comment authentifier l'identité de votre contact Pidgin](#)

---

### 3.0 À propos de Pidgin et d'OTR

Vous et vos correspondants devez configurer le plugin **OTR** pour être en mesure de mener des séances de **messagerie instantanée (MI)** privée et sécurisée. Puisque le plugin a été conçu spécialement pour **Pidgin**, le programme détecte automatiquement **OTR** lorsque les deux parties l'ont correctement installé et configuré.

**N. B.:** Si vous sollicitez une conversation privée auprès d'un contact qui n'a pas installé et configuré **OTR**, le programme envoie automatiquement un message expliquant comment obtenir le plugin **\*\*OTR\***

### 3.1 Comment configurer le plugin Pidgin-OTR

Pour activer le plugin **OTR**, veuillez suivre les étapes énumérées ci-dessous:



**Première étape.** Double-cliquez sur  ou sélectionnez **Démarrer > Programmes > Pidgin** pour lancer **Pidgin** et afficher la fenêtre *Liste des contacts* (voir la *Figure 1*).

**Deuxième étape.** Ouvrez le menu *Outils*, puis sélectionner l'item *Plugins*, comme suit:

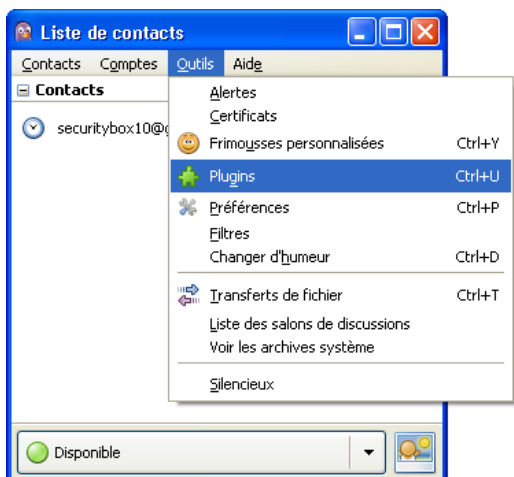


Figure 1: La fenêtre Liste de contacts avec l'item Plugins sélectionné dans le menu Outils

La fenêtre *plugins* s'affiche alors:

**Deuxième étape.** Faites défiler jusqu'à l'option *Messagerie confidentielle Off-the-Record*, puis **cochez** la case adjacente pour l'activer.

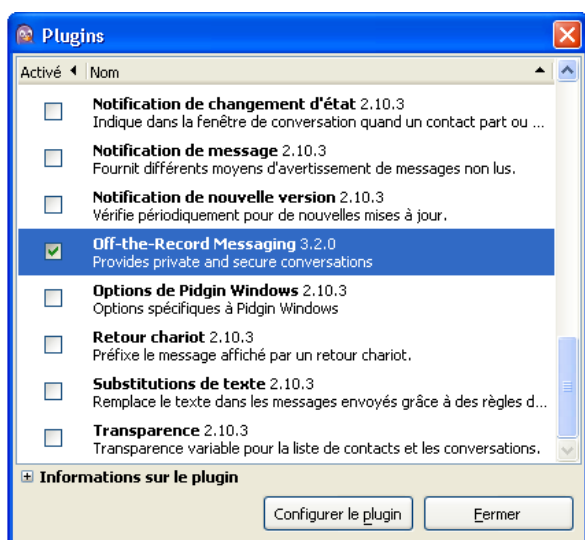


Figure 2: La fenêtre des Plugins de Pidgin avec l'option *Messagerie confidentielle Off-the-Record* sélectionnée

**Troisième étape.** Cliquez sur Configurer le plugin pour configurer la fenêtre *Messagerie confidentielle Off-the-Record*.

Pour résumer, il y a trois étapes de base pour configurer **OTR** correctement et être en mesure de mener des séances de **\*MI\*** privée et sécurisée:

- **La première étape:** Générer une clé privée unique associée à votre compte et afficher son empreinte.

Les deux étapes suivantes consistent à sécuriser votre séance de **MI** et authentifier vos contacts.

- **La deuxième étape:** Une des parties sollicite une séance de messagerie auprès d'un correspondant actuellement en ligne.
- **La troisième mouvement** implique l'*authentification*, c.-à-d. la vérification de l'identité, de votre contact **Pidgin**. (**N. B.:** Dans **Pidgin**, un contact est une personne avec qui vous communiquez lors d'une séance de **MI** La procédure de vérification de l'identité d'un contact est appelé *authentification* dans **Pidgin**. Il s'agit en fait de confirmer que votre contact est *exactement* la personne qu'elle prétend être.

### 3.2 La première étape - Comment produire une clé privée et afficher son empreinte

Les séances de clavardage sécurisées avec **Pidgin** ne sont possibles qu'en créant une *clé privée* pour le compte que vous utilisez. La fenêtre de configuration de *Off-the-Record* comporte deux onglets: *Configuration* et *Empreintes connues*. L'onglet *Configuration* sert à créer une *clé* pour chacun de vos comptes et à régler certaines options d'**OTR**. L'onglet *Empreintes connues* contient les clés de vos contacts. Vous devez disposer d'une clé pour chaque contact avec qui vous souhaitez clavarder de façon privée et confidentielle.

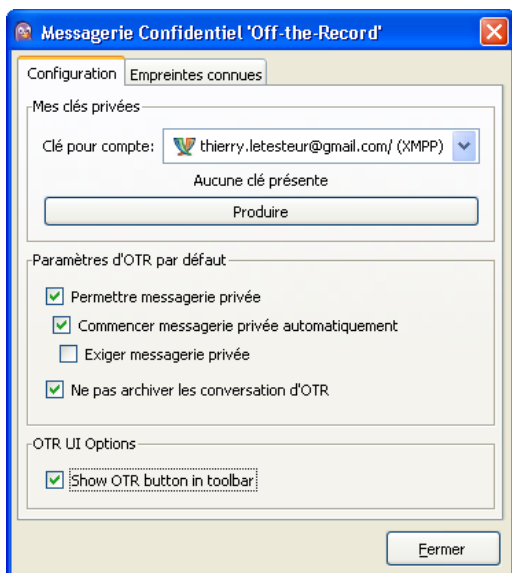


Figure 3: La fenêtre Messagerie confidentielle Off-the-Record affichant le contenu de l'onglet Configuration

**Première étape.** Pour optimiser la confidentialité de vos communications, **cochez** les options *Permettre messagerie privée*, *Commencer messagerie privée automatiquement* et *Ne pas archiver les conversations OTR* dans l'onglet Configuration illustré ci-dessus.

**Deuxième étape.** Cliquez sur  pour créer votre clé. Peu de temps après, une fenêtre apparaît pour vous aviser que la clé privée a bel et bien été créée:

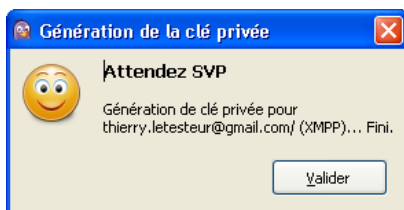


Figure 4: La fenêtre Génération de la clé privée

**N. B.:** Votre contact devra suivre les mêmes étapes dans son propre compte.

**Troisième étape.** Cliquez sur  lorsque la clé privée (qui devrait ressembler à l'illustration ci-dessous) a été créée:

L'empreinte: 13085636 1C803996 C0901931 549EB7A8 72684177

Figure 5: Une exemple d'empreinte de clé privée créée par le moteur OTR

**Important:** Vous venez de créer une clé privée pour votre compte. Cette clé sera utilisée pour chiffrer vos séances de clavardage et faire en sorte que personne ne puisse vous espionner. L'empreinte est une longue séquence de lettres et de chiffres utilisés pour identifier la clé d'un compte, tel qu'illustré à la Figure 5 ci-dessus.

**Pidgin** sauvegarde et vérifie automatiquement votre empreinte et celles de vos contacts pour que vous n'ayez pas à les mémoriser.

### 3.3 La deuxième étape - Comment authentifier une séance de clavardage privée

**Première étape.** Double-cliquez sur le compte d'un de vos contact en ligne pour entamer une nouvelle séance de **MI**. Si vous avez tous les deux installé et correctement configuré le module **OTR**, vous remarquerez qu'un nouvel icône **OTR** est apparu au bas de la fenêtre de clavardage.

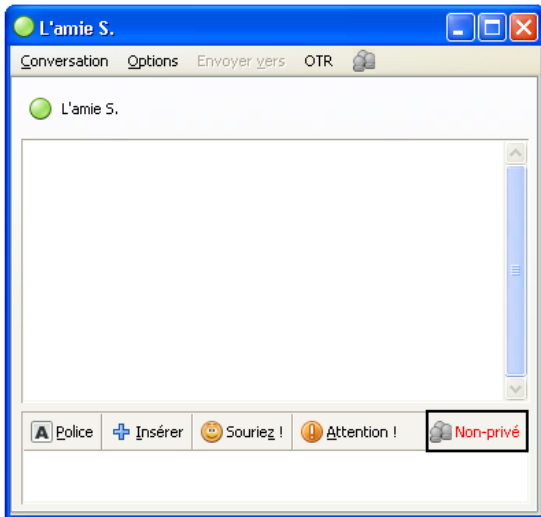



Figure 6: Une fenêtre de messagerie de Pidgin affichant l'icone OTR surligné en noir

**Deuxième étape.** Cliquez sur  pour afficher le menu associé, puis **sélectionnez** l'item *Commencer conversation privée*, tel qu'illustré ci-dessous:

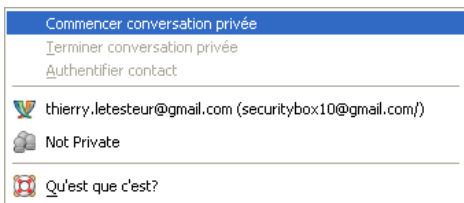


Figure 7: Le menu de l'icone OTR avec l'item *Commencer conversation privée* sélectionné

Votre fenêtre de messagerie **Pidgin** devrait maintenant ressembler à ceci:

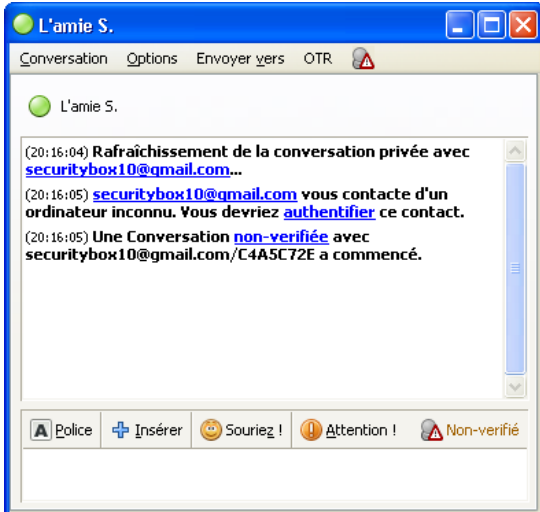




Figure 8: La fenêtre de messagerie de Pidgin affichant le bouton Non-vérifié

**N. B.:** Pidgin communique automatiquement avec le programme de MI de votre contact et affiche un message chaque fois que vous entamez une séance de clavardage privée et sécurisée. En conséquence, le bouton **OTR**  prend maintenant cette allure , ce qui vous indique que vous êtes maintenant prêt à mener une conversation chiffrée avec votre contact.

**Attention!** Même si la conversation est maintenant sécurisée, l'identité de votre contact n'est toujours pas *vérifiée*. Attention: Votre contact pourrait être une tierce personne *usurpant l'identité* de votre contact.

### 3.4 La troisième étape - Comment authentifier l'identité de votre contact Pidgin

Pour authentifier votre contact dans **Pidgin**, vous devrez utiliser l'une des trois méthodes détaillées ci-dessous. Vous pouvez 1) saisir un code ou une phrase secrète déterminée à l'avance avec votre contact; 2) poser un e question dont seulement vous et votre contact connaissez la réponse; 3) vérifiez manuellement vos empreintes respectives en employant un autre mode de communication.



## La méthode par code ou phrase secrète

Vous pouvez vous entendre sur un code secret à l'avance, soit lors d'une rencontre en personne ou en utilisant un autre moyen de communication (comme le téléphone, le téléphone Internet **Skype**, ou un message texte par téléphone cellulaire). Lorsque vous saisissez le même code secret chacun de votre côté, votre séance sera authentifiée.

**N. B.:** La fonction de reconnaissance du code secret dans **OTR** est sensible à la case, c'est-à-dire qu'elle peut faire la différence entre majuscules (A,B,C) et minuscules (a,b,c). Rappelez vous ce détail lorsque vous inventez un code ou une phrase secrète!

**Première étape.** Cliquez sur le bouton *OTR* dans la fenêtre de messagerie, puis **sélectionnez** l'item *Authentifier contact*, comme suit:

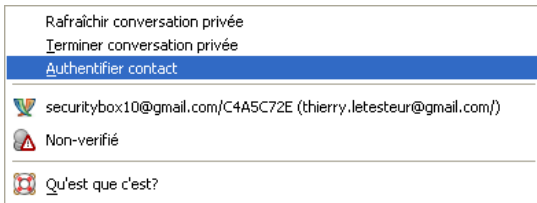


Figure 9: Le menu *Non-vérifié* avec l'item *Authentifier contact* sélectionné

La fenêtre *Authenticate Buddy* s'affiche alors et vous demande de choisir une méthode d'authentification.


**Deuxième étape.** Cliquez sur  et **sélectionnez** l'option *Shared Secret*:



Figure 10: La fenêtre *Authenticate buddy* avec le menu défilant des options de méthodes d'authentification

**Troisième étape.** Saisissez le code ou la phrase secrète, comme suit:

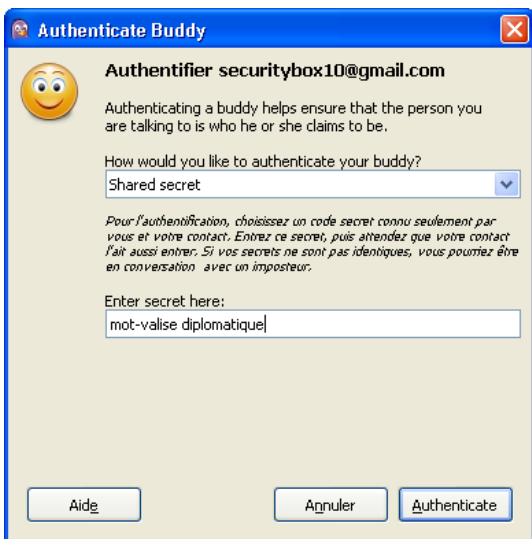
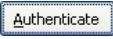


Figure 11: La fenêtre *Shared Secret*

**Quatrième étape.** Cliquez sur  pour afficher la fenêtre suivante:

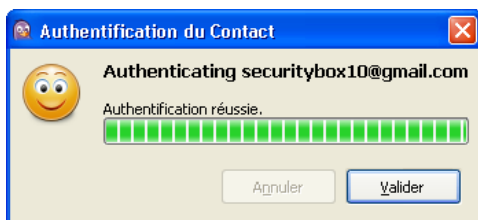



Figure 12: La fenêtre d'authentification d'un correspondant fictif

Si les deux codes correspondent, votre séance sera authentifiée.

**N. B.:** De son côté, votre contact verra la même fenêtre et devra saisir le même code secret. Si les deux codes correspondent, votre séance sera authentifiée.



Figure 13: La fenêtre Authenticate Buddy d'un correspondant fictif

Lorsque la séance est authentifiée, le bouton OTR s'affiche comme ceci: . Votre séance de clavardage est désormais sécurisée et vous êtes assuré que la personne avec qui vous correspondez est bel et bien votre contact.

## La méthode par question et réponse

Une autre façon d'authentifier vos contacts est la méthode par question et réponse. Créez une question et une réponse correspondante. Après avoir lu votre question, votre contact doit saisir *exactement* la même réponse, et si les deux réponses correspondent, votre identité sera automatiquement authentifiée.

**Première étape.** Cliquez sur le bouton OTR dans une fenêtre de messagerie active pour afficher le menu correspondant, puis sélectionnez l'item *Authentifier contact* (voir la Figure 9).

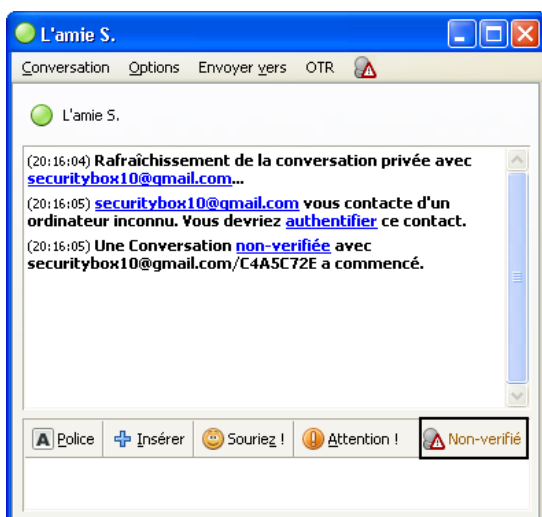


Figure 14: Une fenêtre de messagerie Pidgin affichant l'icone OTR

Une fenêtre *Authentifier contact* s'affiche alors et vous demande de choisir une méthode d'authentification.

**Deuxième étape.** Cliquez sur le menu défilant et sélectionnez la méthode *Question and Answer*:

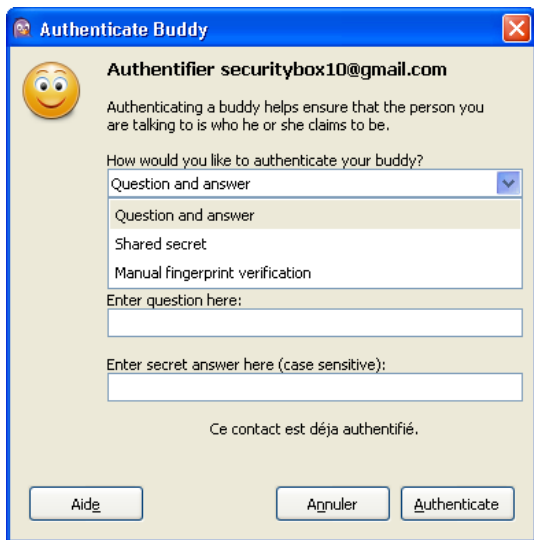



Figure 15: La fenêtre Authenticate Buddy

**Troisième étape.** Saisissez une question et la réponse correspondante. La question sera automatiquement envoyée à votre contact.



Figure 16: La fenêtre Question et réponse

Si la réponse de votre contact correspond à la vôtre, vos identités seront mutuellement authentifiées, et les deux parties sont bel et bien qui elles prétendent être!

Lorsque la séance sera authentifiée, le bouton OTR ressemblera à ceci . Votre séance est maintenant sécurisée et vous êtes assuré de l'identité de votre contact.

Remarquez que lorsque vous **Sélectionnez > Liste de contacts > Outils > Plugins > Messagerie confidentielle Off-The-Record > Configurer le plugin**, l'onglet *Empreintes connues* affiche désormais le compte de votre contact et un message indiquant que son identité a été vérifiée.

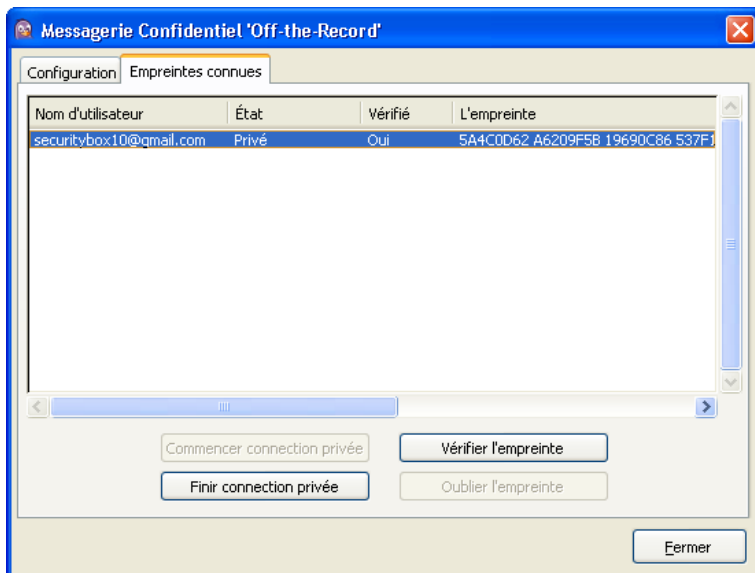


Figure 17: La fenêtre Messagerie confidentielle Off-the-Record Messaging affichant les empreintes connues

Félicitations! Vous pouvez maintenant clavarder en tout confidentialité. La prochaine fois que votre contact et vous voudrez clavarder (en utilisant les mêmes ordinateurs), vous pourrez sauter les étapes 1 et 2 décrites ci-dessus. Vous n'aurez qu'à demander une connexion sécurisée et votre contact n'aura qu'à l'accepter.

## Comment créer un compte Google Talk

Sommaire des sections de cette page:

- [4.0 Comment créer un compte Google Talk](#)
- [4.1 Comment activer une connexion sécurisée](#)

### 4.0 Comment créer un compte Google Talk

Pour créer un compte **Google talk** (qui emploie le protocole **XMPP**) vous devez d'abord créer un compte **Gmail**.

Pour créer un compte **Gmail**, veuillez suivre les étapes énumérées ci-dessous:

**Première étape.** Ouvrez votre navigateur Internet, puis saisissez <http://www.google.com> <sup>[158]</sup> dans la barre d'adresse du navigateur pour afficher la page d'accueil \*\*Google\*:

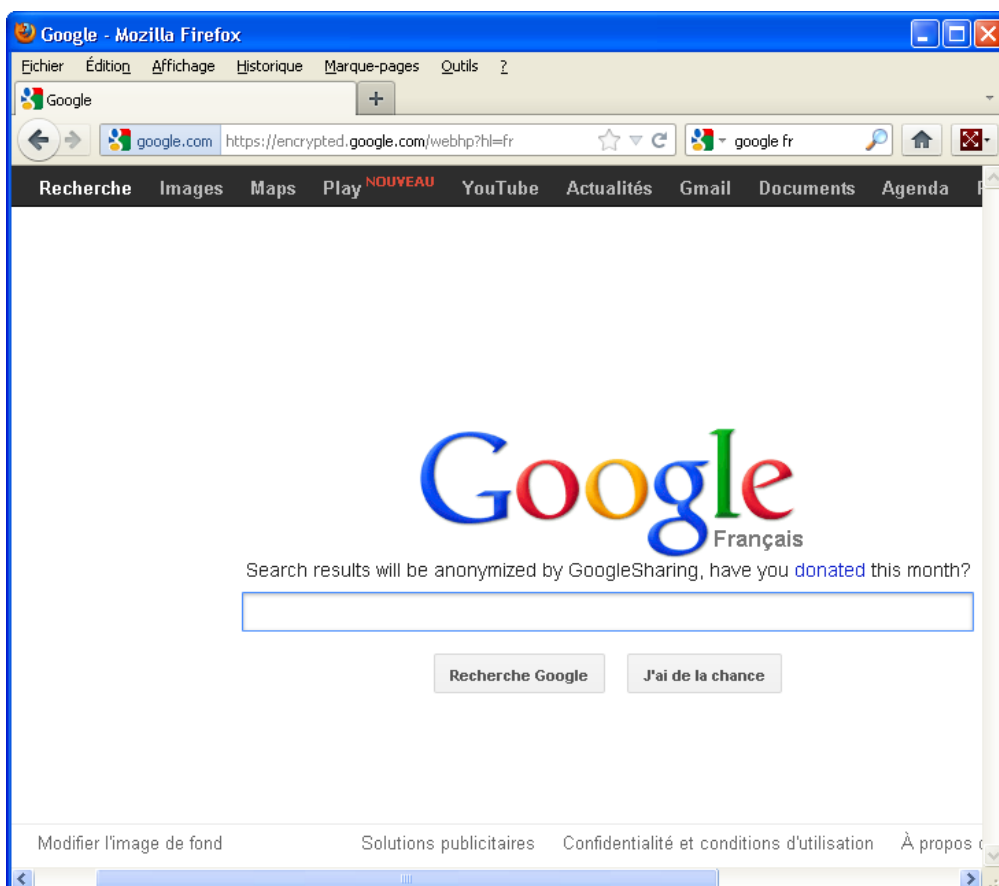


Figure 1: Un exemple de page d'accueil de Google

Deuxième étape. Cliquez sur le lien **Gmail** (surligné en rouge) dans le menu principal, tel qu'illustré ci-dessous:



Figure 2: Le menu principal de la page d'accueil de Google avec le lien Gmail surligné

Cela active la fenêtre suivante:

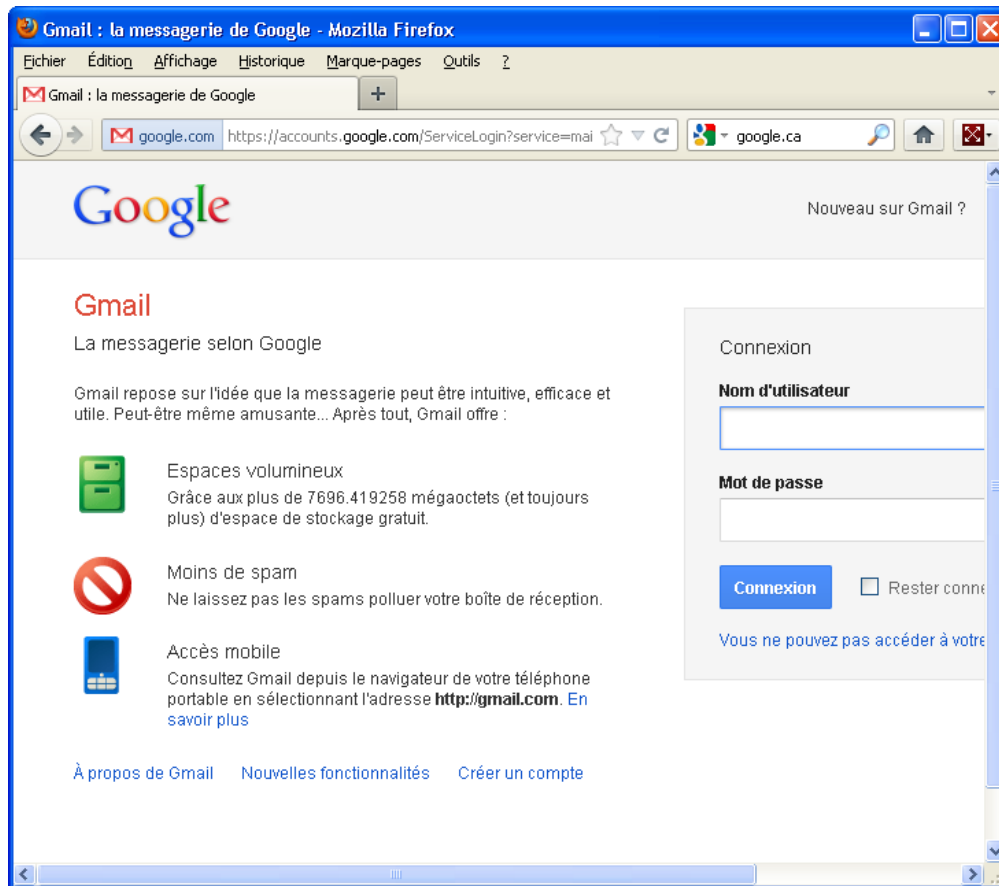


Figure 3: La page d'accueil Gmail

Troisième étape. Cliquez sur **CRÉER UN COMPTE** pour afficher la fenêtre suivante:

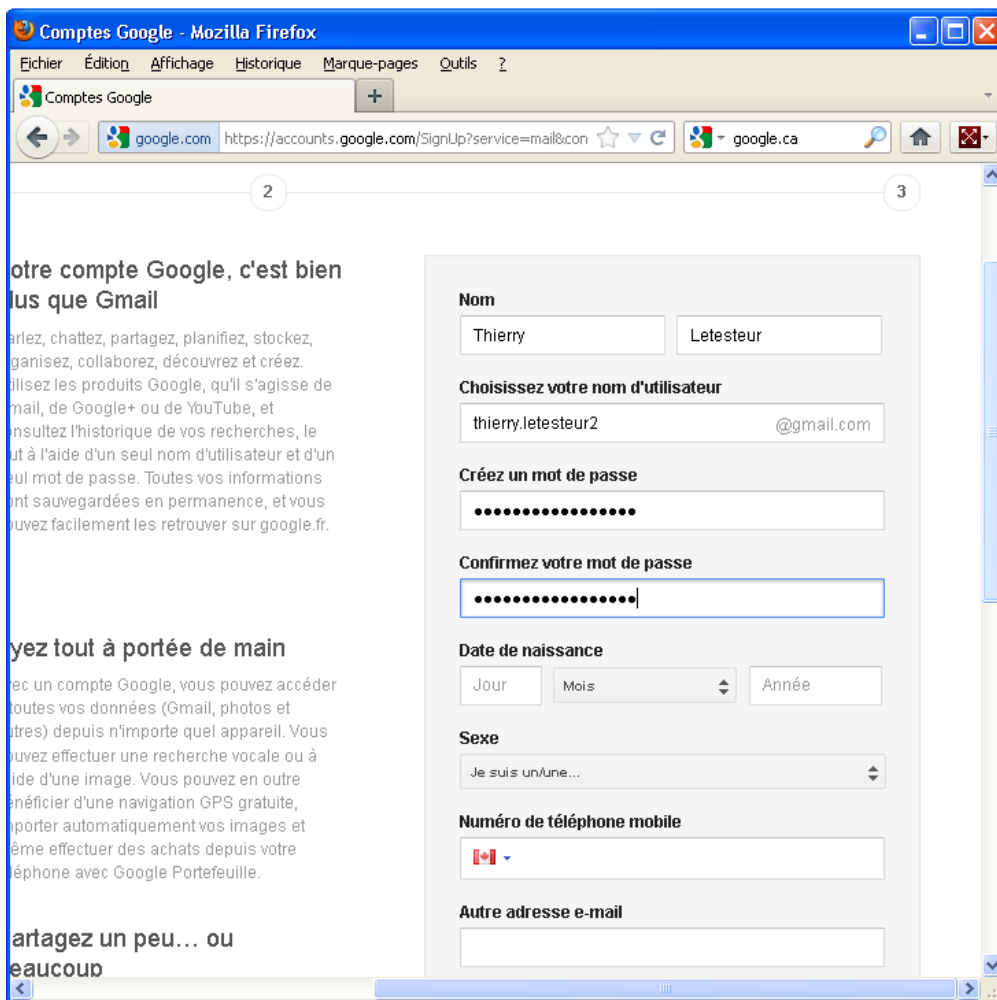


Figure 4: La première partie du formulaire de création d'un compte Gmail

**N. B.:** Le formulaire de création d'un compte Gmail est trop long pour être reproduit au complet, et est divisé en deux sections essentielles dans cet exemple. Comme toujours, moins vous fournissez de renseignements personnels, plus la confidentialité et la sécurité de vos communications seront protégées.

**Quatrième étape. Saisissez** les renseignements requis dans les zones de texte *Prénom*, *Nom* et *Nom d'utilisateur*. Pour préserver votre anonymat, ces renseignements ne devraient pas correspondre à vos vrais nom et prénom.

**Cinquième étape.** Gmail vérifie automatiquement la disponibilité du nom d'utilisateur que vous avez saisi. S'il n'est pas disponible, essayez quelque chose d'un peu plus original!

**Sixième étape. Désactivez** les options *Rester connecté* et *Activer l'histoire Web*. (N. B. Dans les versions plus récentes du formulaire, ces options ont été éliminées. Vous pouvez donc poursuivre normalement la procédure de création du compte.)

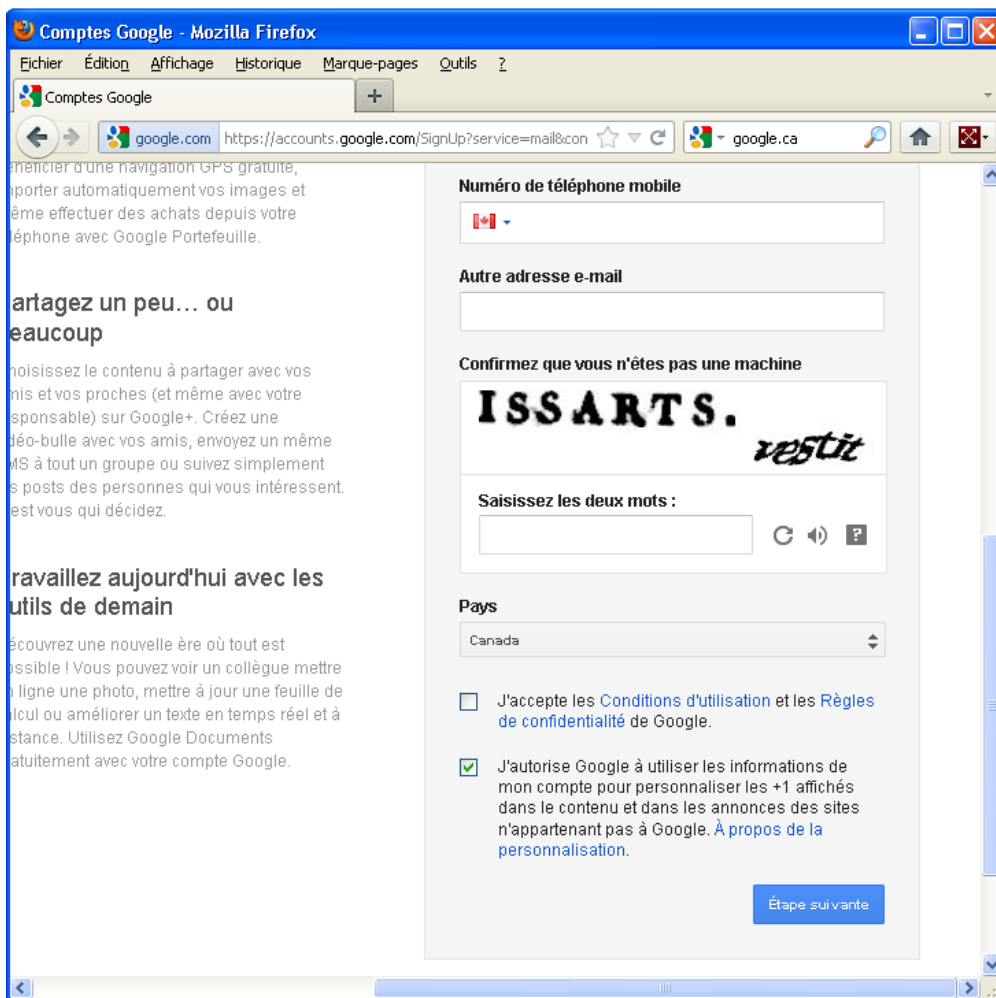


Figure 5: La deuxième partie du formulaire de création d'un compte Gmail

**Septième étape.** Saisissez les autres renseignements requis.

**Huitième étape.** Sélectionnez le pays qui correspond à votre emplacement dans la liste défilante *Pays*.

**N. B.:** Un niveau encore plus élevé de confidentialité est possible si vous avez l'occasion de créer un compte **Gmail** lorsque vous vous trouvez dans un pays qui n'est pas votre pays d'origine ou de résidence permanente.

**Neuvième étape.** Saisissez les mots déformés dans la zone de texte pour confirmer que ce n'est pas une machine qui tente de créer ce compte!

**Dixième étape.** Cochez la case *J'accepte les conditions d'utilisation et les règles de confidentialité de Google*, décochez la case *J'autorise Google à utiliser les informations de mon compte...*, puis cliquez sur **Étape suivante** pour accepter les conditions d'utilisation de **Google** et afficher la page suivante.

**Onzième étape.** Cliquez à nouveau sur **Étape suivante** (N. B. Pour préserver votre anonymat, il est contre-indiqué de fournir une photo ou un portrait de vous sur Internet.)



## Bienvenue Thierry !

Vous pouvez désormais commencer à effectuer des recherches, à créer et à partager vos contenus sur de nombreux produits Google. Découvrez votre nouveau compte dans l'angle supérieur droit : cliquez sur votre photo pour modifier votre profil, accéder à Google+, et consulter et modifier les paramètres de votre compte et de votre historique Web. Nous vous avons également envoyé un e-mail pour vous expliquer comment tirer le meilleur parti de Google.

Votre nouvelle adresse e-mail est [thierry.letesteur2@gmail.com](mailto:thierry.letesteur2@gmail.com).

Merci d'avoir créé un compte. Amusez-vous bien !

**Poursuivre vers Gmail**

Figure 6: La page d'introduction de Gmail

Félicitations! Vous avez créé un compte **Gmail** ainsi qu'un compte **Google Talk** en remplissant le minimum requis de

zones de texte et en ne fournissant aucun renseignement superflu. Maintenant que vous disposez d'un compte **Google Talk**, vous êtes prêt à l'inscrire dans **Pidgin**. Pour en apprendre davantage sur l'enregistrement d'un compte dans **Pidgin**, veuillez vous référer à la section **Comment enregistrer votre compte de messagerie instantanée dans Pidgin** [159]. Lorsque vous aurez complété la procédure d'enregistrement de votre compte **Gmail** dans **Pidgin**, revenez à la section suivante pour apprendre comment activer une connexion sécurisée.

## 4.1 Comment activer une connexion sécurisée

Les utilisateurs qui enregistrent dans **Pidgin** un compte **Google Talk**, **IRC**, **SILC**, ou tout service compatible avec le protocole **XMPP**, peuvent configurer **Pidgin** pour utiliser une connexion sécurisée, aussi connue comme *Secure Socket Layer (SSL)* ou *Transport Layer Security (TLS)*.

Pour configurer une connexion **SSL** ou **TLS**, veuillez suivre les étapes énumérées ci-dessous:



**Première étape.** Cliquez sur **Pidgin** ou sélectionnez **Démarrer > Pidgin** pour lancer **Pidgin** et afficher la *Liste de contacts*.

**Deuxième étape.** Ouvrez le menu *Comptes* et sélectionnez votre compte pour activer le menu correspondant, puis sélectionnez l'item *Modifier le compte*:

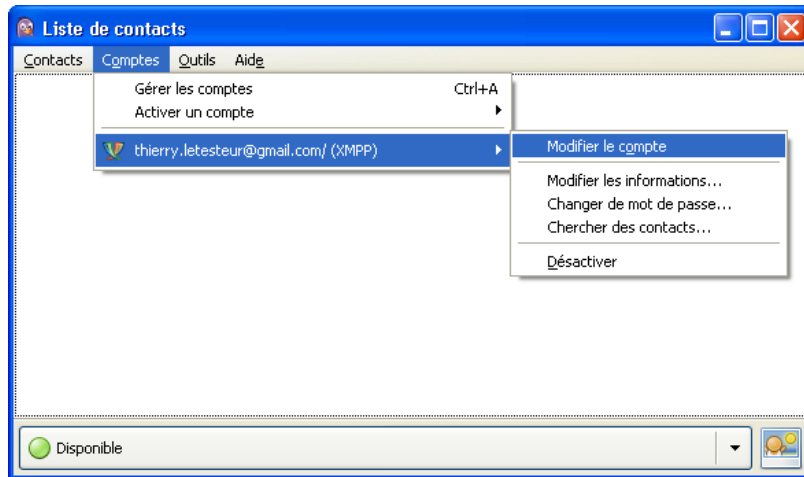


Figure 7: Le menu *Comptes* affichant un compte **Pidgin** avec l'item *Modifier compte* sélectionné

Cela active la fenêtre *Modification du compte* et affiche le contenu de l'onglet *Essentiel*:

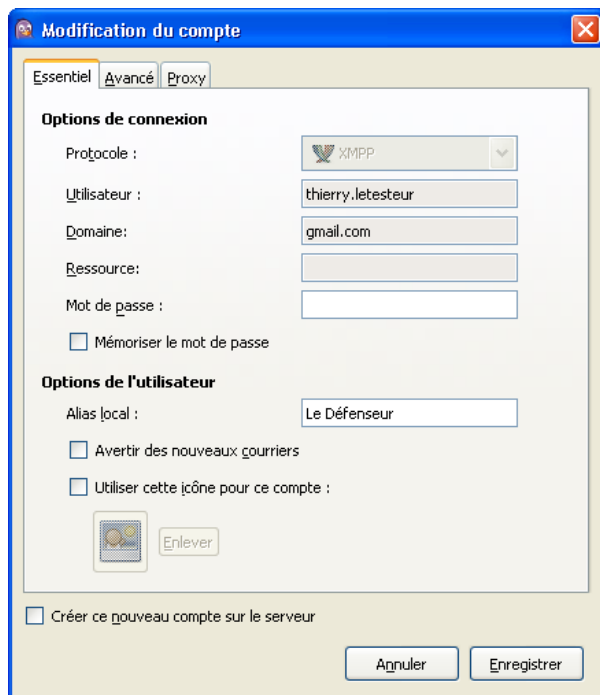


Figure 8: La fenêtre *Modification du compte* affichant le contenu de l'onglet *Essentiel*

**N. B.:** Si vous avez déjà un compte **Gmail** enregistré dans **pidgin**, la fenêtre *Modification du compte* s'affichera comme à la Figure 8 ci-dessus.

**Troisième étape.** Cliquez sur l'onglet *Avancé* pour le configurer comme suit:



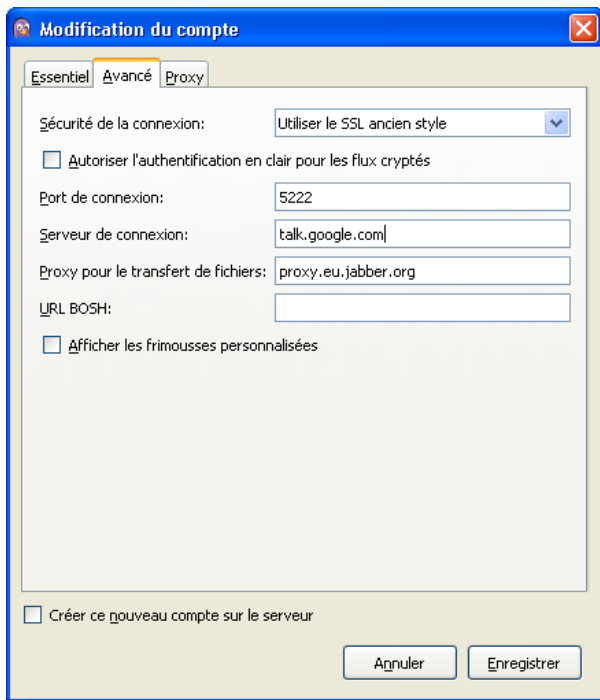


Figure 9: La fenêtre Modification du compte affichant le contenu de l'onglet Avancé

**Quatrième étape.** Sélectionnez l'option *Utiliser le SSL ancien style* pour activer automatiquement une voie de communication sécurisée à chaque séance de messagerie instantanée.

**Cinquième étape.** Saisissez *talk.google.com* dans la zone de texte *Serveur de connexion*.

**Sixième étape.** Cliquez sur  pour enregistrer vos réglages, puis cliquez sur l'onglet *Proxy*:



Figure 10: La fenêtre Modification du compte affichant le contenu de l'onglet Proxy

**Septième étape.** Sélectionnez l'option *Utiliser les paramètres proxy globaux* si ce n'est pas déjà l'option par défaut, puis cliquez sur  pour activer une connexion sécurisée entre vous et votre correspondant.

## Faq et questions récapitulatives

### 5.0 Faq et questions récapitulatives

Claudia et Pablo ont tous deux réussi à installer et configurer **Pidgin** et le moteur de chiffrement et d'authentification **OTR**. Les deux ont passé quelques heures à explorer les différentes options et à expérimenter en clavardant ensemble avec leurs comptes **Google Talk** et leurs autres comptes utilisant les différents protocoles de **MI** supportés par **Pidgin**.

Toutefois, Pablo a encore quelques questions à propos de **Pidgin-OTR**.

**Q:** Est-ce que je peux utiliser **Pidgin-OTR** pour clavarder avec des amis dans **MSN** et **Yahoo**?

**\*R:** Même si **Pidgin-OTR** est compatible avec bon nombre de services de messagerie et de clavardage, toi et ton contact devez utiliser le même fournisseur de service pour lancer une séance de **MI**. Vous devez tous deux utiliser un compte **MSN** ou un compte **Google Talk**, par exemple. Cependant, dans **Pidgin** tu peux être enregistré et connecté avec plusieurs comptes de **MI** simultanément. C'est l'avantage principal d'un client de **MI** multi-protocole.

**Q:** Comment puis-je accéder à mon compte **Pidgin-OTR** à partir d'un autre ordinateur?

**R:** Il te faudrait créer une nouvelle clé privée pour utiliser ton compte de **MI** sur cet ordinateur. Tu peux entamer une conversation avec ton contact en utilisant cette nouvelle clé, mais tu devras authentifier ta séance de nouveau.

**Q:** Qu'advient-il si j'oublie mon mot de passe pour mon compte de **MI**? Ou si quelqu'un le vole? Cette personne aura-t-elle accès à mes conversations passées et futures?

**R:** C'est une **excellente** question, et très importante. Premièrement, si tu oublies ton mot de passe d'enregistrement, tu devras créer un nouveau compte de **MI**. Ensuite, tu devras aviser ton contact de la création de ce nouveau compte par téléphone, **Skype**, téléphonie Internet, ou courriel sécurisé.


Enfin, toi et tes contacts devrez vous authentifier de nouveau. Si une personne a obtenu ton mot de passe de **MI**, elle pourrait essayer de se faire passer pour toi en utilisant **Pidgin**. Heureusement, elle ne pourrait pas authentifier la séance puisque toi seul connais le code secret que tu partages avec ton contact. Dans ce cas-là, ton contact devrait avoir la puce à l'oreille. C'est pourquoi l'authentification est tellement importante. De plus, si tu as suivi pas à pas les consignes et adéquatement configuré **OTR** avec les préférences recommandées, même si une personne te vole ton mot de passe, elle n'aura pas accès à tes conversations passées, puisque tu as choisi de ne pas les archiver.

## 5.1 Questions récapitulatives

- Combien de fois est-il nécessaire d'authentifier une séance de clavardage avec un contact donné?
- Est-il possible d'enregistrer et utiliser plusieurs compte de messagerie instantanée simultanément **Pidgin**?
- Qu'est-ce qu'une empreinte, dans **Pidgin**?
- Qu'advient-il de vos préférences **OTR** (y compris les empreintes reçues) lorsque vous installez **Pidgin-OTR** sur un autre ordinateur?
- Quels sont les configurations requises pour initier une séance de clavardage sécurisée et confidentielle dans **Pidgin**?
- Quelles sont les configurations requises pour créer d'un compte dans **Pidgin**?

## VaultletSuite - client de courriel sécurisé

**VaultletSuite 2 Go (VS2Go)** est un programme de courrier électronique sécurisé qui vous donne la possibilité de stocker vos messages de courriel et autres fichiers sur votre ordinateur, sur une clé USB ou sur le serveur de VaultletSoft.

<b>Site Internet</b> <a href="http://www.vaultletsoft.com">www.vaultletsoft.com</a> <sup>[160]</sup>	<b>Pour installer VaultletSuite</b> <ul style="list-style-type: none"><li>• Lisez la courte introduction des <u>Guides pratiques</u> <sup>[89]</sup></li><li>• <b>Cliquez sur l'icône ci-dessous et 'Ouvrez' ou 'Exécutez' l'assistant d'installation.</b> Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.</li><li>• Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.</li></ul>
<b>Configuration requise :</b> <ul style="list-style-type: none"><li>• Windows 2000/XP/Vista</li><li>• Une connexion Internet</li></ul>	
<b>Version utilisée pour rédiger ce guide :</b> <ul style="list-style-type: none"><li>• 2.7.9 (peut différer)</li></ul>	
<b>Licence :</b> <ul style="list-style-type: none"><li>• Gratuiticiel (Freeware)</li></ul>	<b>VaultletSuite:</b>  <sup>[161]</sup>

**Lecture préalable :**

- Livret pratique Security in-a-box, chapitre 7. Préserver la confidentialité de vos communications sur Internet <sup>[162]</sup>.

**Niveau :** 1 : Débutant, 2 : Moyen, 3 : Intermédiaire, 4 : Expérimenté, 5 : Avancé

**Temps d'apprentissage :** 60 minutes

**Ce que vous apportera l'utilisation de cet outil :**

- Un programme de courrier électronique sécurisé, qui chiffre automatiquement vos messages et fichiers.
- La capacité de déterminer comment vos messages de courriel sont lus par le(s) destinataire(s). Par exemple, vous pouvez faire en sorte qu'il soit impossible de transférer les courriels que vous envoyez à d'autres destinataires, ou encore configurer les messages pour qu'ils soient automatiquement supprimés après la première lecture.
- La possibilité d'envoyer des messages chiffrés à n'importe quelle adresse de courriel, sans qu'il soit nécessaire pour vos destinataires d'utiliser VaultletSoft ou un autre outil particulier pour les lire.
- La capacité de transporter avec vous vos messages et fichiers en les stockant de façon sécurisée sur une clé USB.

### 1.1 À propos de cet outil

**VaultletSuite 2 Go (VS2Go)** est un programme de courrier électronique sécurisé qui vous donne la possibilité de stocker vos messages de courriel et autres fichiers sur votre ordinateur, sur une clé USB ou sur un serveur de VaultletSoft. Pour fonctionner normalement, VS2Go doit installer la plateforme **Java** sur votre ordinateur. Ce logiciel a une apparence un peu différente des autres programmes de messagerie avec lesquels vous êtes déjà familier, et votre compte de courriel n'est pas accessible via un navigateur Internet.

VS2Go est une suite logicielle composée de trois produits complémentaires, accessibles par une console unique :

- **VaultletMail** – le client de messagerie
- **PasswordValet** – l'outil de gestion des mots passe
- **VaultletFiler** – l'outil de chiffrement des fichiers

VS2Go utilise la méthode de chiffrement asymétrique (par clé publique) pour assurer la sécurité de vos communications et de vos données. Vous pouvez en apprendre davantage sur cette méthode de chiffrement en lisant le chapitre 7, [Préserver la confidentialité de vos communications sur Internet](#) [162] du livret pratique. Toutes les tâches de chiffrement sont effectuées automatiquement pour vous par le logiciel VS2Go. Cela accroît le niveau de sécurité de vos communications en réduisant le facteur d'erreur humaine, tout en facilitant l'utilisation du programme.

VS2Go offre un peu d'espace sur ses serveurs pour vos messages de courriel. Les nouveaux messages y seront stockés et pourront être relevés à partir de n'importe quel ordinateur où le logiciel VS2Go est installé. Néanmoins, vous devriez créer une archive locale sur votre ordinateur ou sur une clé USB et y transférer régulièrement vos messages. L'archive locale n'est limitée que par son volume.

#### Offline Installation Instructions :

##### Pour installer VaultletSuite

- \*Lisez la courte **Introduction** aux **Guides pratiques** [1]\*\*
- **Cliquez sur l'icône VaultletSuite ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.

VaultletSuite:




[163]

## Comment créer un compte VS2Go

**Commentaire sur l'installation** : Après avoir installé VS2Go et lancé le programme une première fois, il est possible que vous receviez des requêtes de mise à jour vous invitant à installer la plus récente version. Veuillez consulter la section 2.3 **Sur l'actualisation de VS2Go** pour connaître la procédure à suivre lorsque cela se produit.

Votre compte VS2Go comprend une adresse de courriel et des renseignements de connexions pour le système. Vous pouvez enregistrer plusieurs comptes sur le même ordinateur. Chaque compte dispose d'un espace séparé et est protégé contre les accès de non propriétaires.

**Première étape.** Cliquez sur :  ou sélectionnez : **Démarrer > Programmes > VaultletSuite2Go > VaultletSuite2Go** pour activer la console principale de *VaultletSuite 2 Go* et la fenêtre *Bienvenue à VaultletSuite 2 Go* :

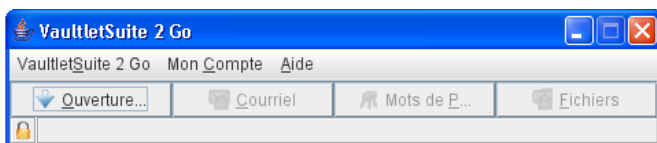


Figure 1 : La console principale de VaultletSuite 2 Go

La console de VS2Go vous permet de naviguer entre le programme de courriel, l'outil de stockage de fichiers et l'outil de gestion de mots de passe de VaultletSuite. Vous devez toutefois créer un compte avant de pouvoir commencer à utiliser ces outils.

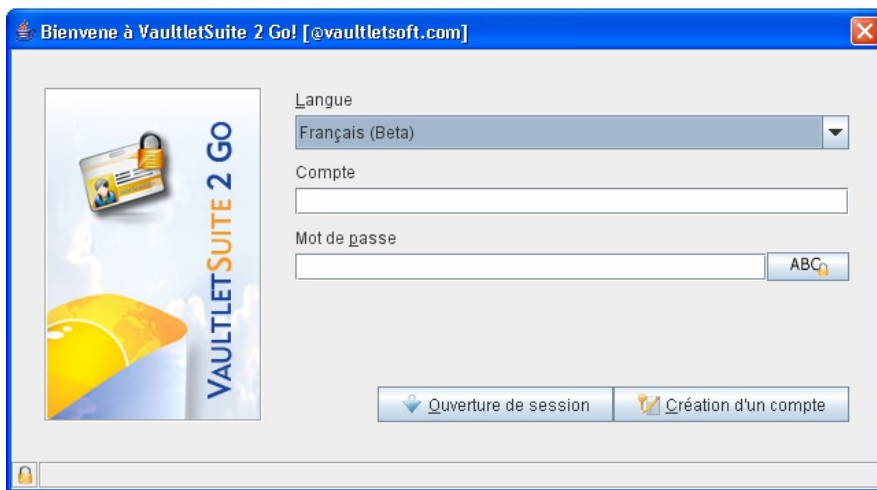


Figure 2 : La fenêtre Bienvenue à VaultletSuite 2 Go

Deuxième étape. Cliquez sur :  pour afficher la fenêtre suivante.

La fenêtre *Choisissez le mode de création de compte que vous souhaitez utiliser* est abordée plus en détails à la prochaine section.

## 2.1 Comment choisir le bon compte VS2Go

VaultletSuite vous offre la possibilité de stocker votre compte et vos renseignements de connexion sur votre ordinateur ou sur une clé USB. Cette option sert à accommoder aussi bien les personnes qui utilisent toujours le même ordinateur que celles qui utilisent plusieurs ordinateurs différents, et ce, sans pour autant compromettre leur sécurité.

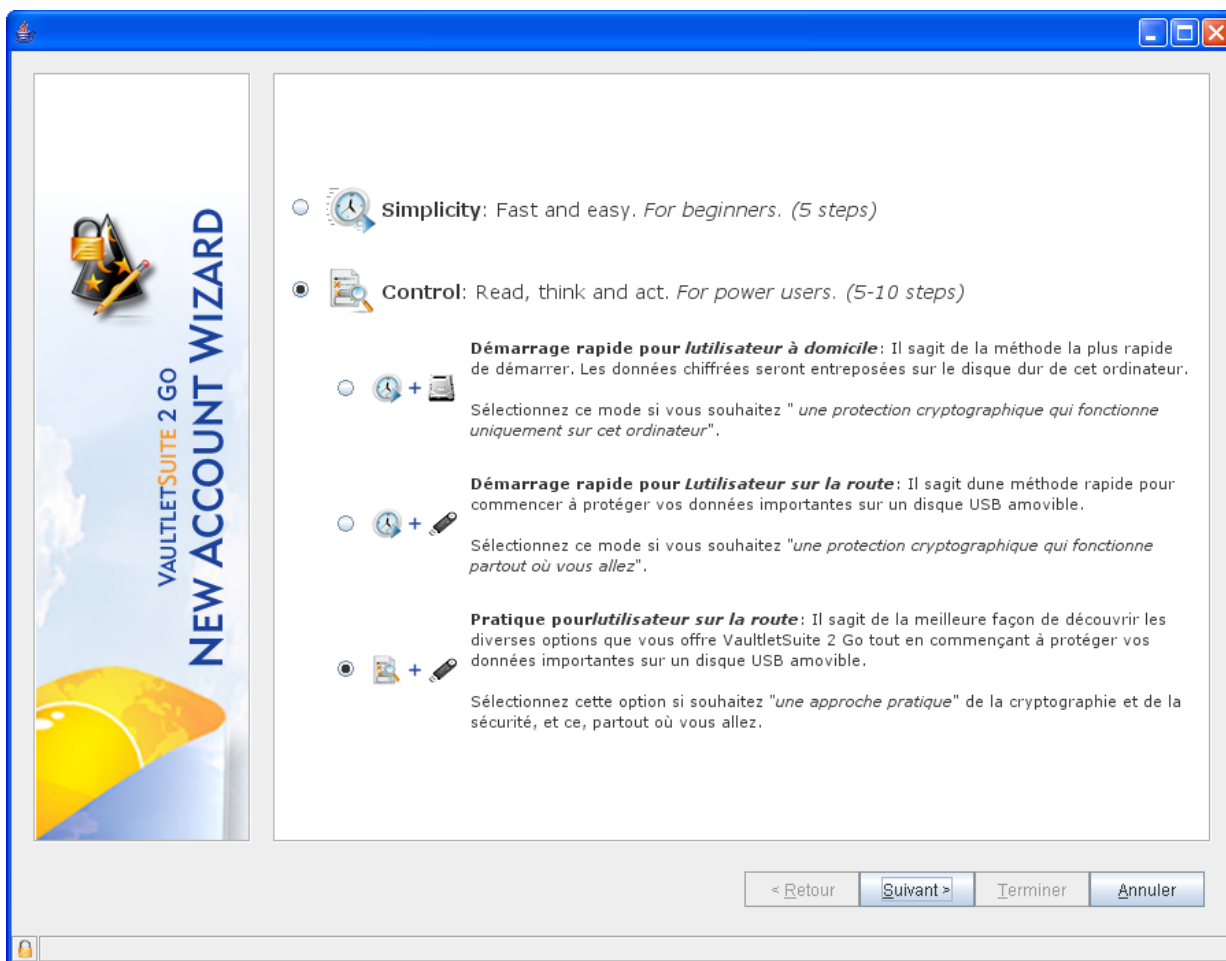


Figure 3 : La fenêtre Choisissez le mode de création de compte que vous souhaitez utiliser

**Important :** Veuillez lire les descriptions des différentes options avant de choisir celles qui correspondent le mieux à vos besoins.

- L'option *Simplicité. Rapide et facile. Pour débutants* est appropriée pour les utilisateurs qui sont satisfaits avec les options par défaut lors de l'enregistrement du compte. Vous devrez fournir un minimum de renseignements. Le compte sera stocké dans le répertoire 'home' de votre ordinateur (par exemple - C:\Documents and Settings\User\vaultletsoft) et la clé privée sera stockée sur le serveur de VaultletSoft.
- L'option *Contrôle: Démarrage rapide pour l'utilisateur à domicile* crée un compte par la même procédure de

configuration qu'avec l'option *Simplicité*, mais donne davantage de détails sur les choix liés à l'installation et à l'accès au système.

- L'option *Contrôle: Démarrage rapide pour l'utilisateur sur la route (6 étapes)* est conçu pour faciliter un processus d'enregistrement rapide, en tenant pour acquis que vos courriels et fichiers seront sauvegardés sur une clé USB. Choisissez cette option si vous souhaitez transporter votre compte VS2Go avec vous et y accéder à partir de plusieurs ordinateurs différents.
- L'option *Contrôle: Pratique, pour l'utilisateur sur la route (10 étapes)* est appropriée pour les utilisateurs qui veulent étudier attentivement toutes les options avant de choisir la configuration qui leur convient le mieux. Vous pouvez aussi choisir l'emplacement où sera stockée votre clé privée.

**Commentaire :** Dans le présent guide, nous ferons la démonstration d'un enregistrement avec l'option *Pratique pour l'utilisateur sur la route*, avec des réglages qui seront appropriés pour la plupart des utilisateurs. Pour ceux qui préfèrent choisir un autre mode d'enregistrement de compte, veuillez tout de même étudier attentivement la prochaine section pour avoir une meilleure idée des étapes importantes.

**Première étape.** Sélectionnez le mode de création de compte qui convient le mieux à vos besoins.

**Deuxième étape.** Cliquez sur : 

## 2.2 Procédure d'enregistrement pas à pas

Cette section fait la démonstration d'un enregistrement d'un compte VS2Go avec l'option *Pratique pour l'utilisateur sur la route*.

Pour commencer, il vous faut générer votre paire de clés. Ce sera la principale mesure de sécurité de votre compte.

**Première étape.** Rattrapez le carré coloré avec votre souris!

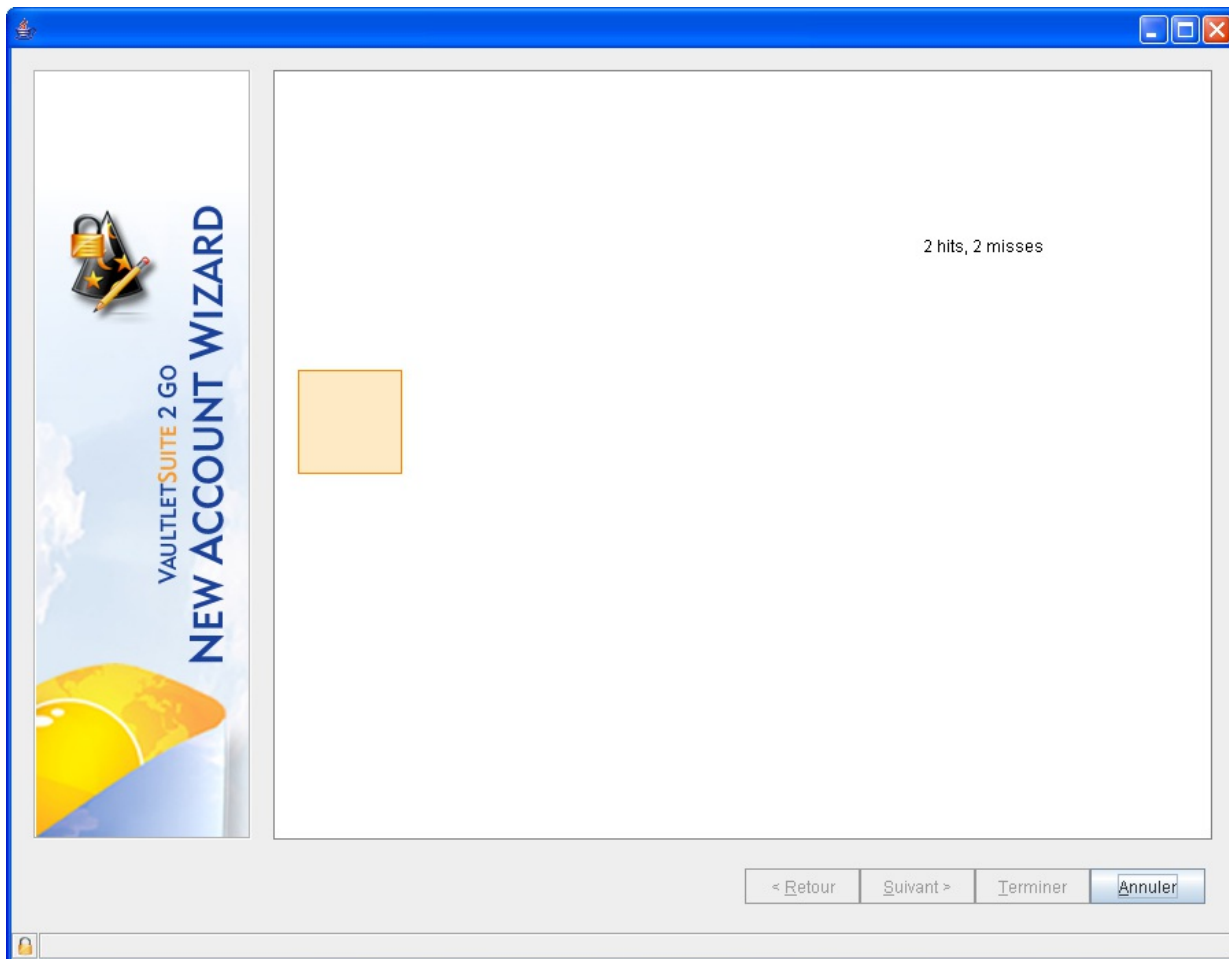


Figure 4 : La fenêtre du générateur de paires de clé

**Deuxième étape.** Choisissez un emplacement où stocker votre clé privée.

**Commentaire :** N'oubliez pas que votre clé privée est le seul moyen dont vous disposez pour déchiffrer les messages et les fichiers dans votre compte. Si vous choisissez de la sauvegarder localement (l'option *Contrôle*, voir ci-dessus) -- sur votre ordinateur ou sur une clé USB -- assurez-vous de ne pas perdre ou endommager ce fichier. Il ne vous sera pas possible de remplacer votre clé privée si vous perdez ou endommagez l'originale. Cette option est appropriée pour les utilisateurs expérimentés qui sont confiants d'être en mesure de gérer leur clé privée de façon sûre. Si vous décidez de sauvegarder votre clé privée sur les serveurs de VaultletSoft (l'option *Simplicité*, voir ci-dessus), vous n'aurez plus à vous soucier de la perdre ou d'en conserver une copie chaque fois que vous souhaitez accéder à votre compte. La responsabilité de conserver votre clé privée reposera sur la compagnie VaultletSoft. Par contre, dans ce dernier scénario, vous devrez créer une phrase secrète exceptionnellement longue afin de protéger votre clé. Pour plus de renseignements sur les clés publiques et privées, veuillez consulter le chapitre 7. Préserver la confidentialité de vos communications sur Internet <sup>[162]</sup> du livret pratique.

Troisième étape. Sélectionnez l'option *Simplicité*

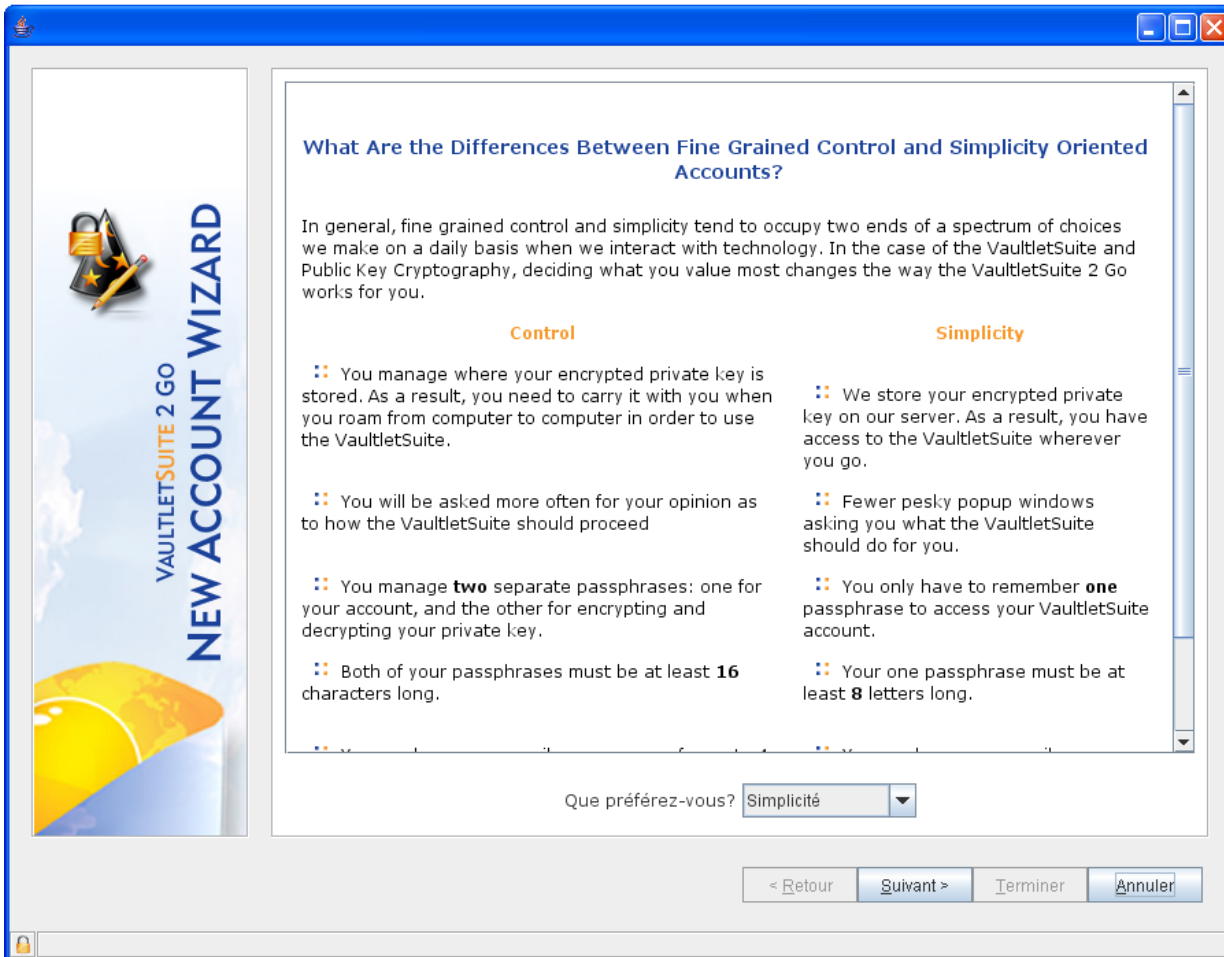


Figure 5: Choisissez un mode d'enregistrement

Quatrième étape. Cliquez sur :  pour continuer.

Il est possible que vous voyiez apparaître une fenêtre vous présentant la licence gratuite pour les organismes à but non lucratif. La prochaine fenêtre est celle de l'enregistrement du compte. Choisissez un nom pour le compte et une phrase secrète (mot de passe), et saisissez les autres renseignements demandés.

**Pour l'instant, VaultletSuite 2 Go est un service en ligne. Il vous faut créer un compte pour l'utiliser.**

Même s'il n'est **pas nécessaire** de fournir votre adresse de courriel actuelle, cela nous aide à communiquer avec vous lorsque nous effectuons des opérations de maintenance du système, ajoutons de nouvelles fonctionnalités et désirons vous informer des derniers développements de VaultletSoft, ou lorsque vous devez réinitialiser votre mot de passe.

Pour plus de renseignements, veuillez cliquer sur le bouton "Confidentialité" ci-dessus pour consulter notre politique de confidentialité.

**Nota Bene:** au lieu de nous donner une adresse de courriel inexistante ou inaccessible parce qu'elle est perpétuellement remplie à capacité, nous préférons que vous ne donniez aucune adresse.

Votre prénom:

Votre nom de famille:

Votre adresse de courriel actuelle (optionnelle):

Nom d'utilisateur souhaité (par ex. 'votre.nom'):

Votre mot de passe:

Votre mot de passe (répétez):

Indicateur de la longueur du mot de passe:

< Retour   Suivant >   Terminer   Annuler

Les mots de passes coïncident!

Figure 6 : Le formulaire de création de compte

**Cinquième étape. Saisissez** les renseignements requis dans les zones appropriées.

**Votre adresse de courriel actuelle** sera utilisée pour réinitialiser votre phrase secrète ou pour vous communiquer des annonces importantes concernant votre compte.

**Commentaire :** Si vous souhaitez accroître le niveau d'anonymat de votre compte VS2Go, vous pouvez enregistrer un nom fictif et omettre l'adresse de courriel alternative. N'oubliez pas, cependant, que si vous n'indiquez pas d'adresse de courriel de rechange, vous ne serez pas en mesure de réinitialiser votre phrase secrète (mot de passe) si vous l'oubliez ou la perdez.

Votre **Nom d'utilisateur souhaité** ne doit pas contenir d'espaces et doit être complètement original. Ce nom sera utilisé dans votre adresse de courriel VS2Go. *Par exemple :* [terrence.letesteur@vaultletsoft.com](mailto:terrence.letesteur@vaultletsoft.com) <sup>[164]</sup>

**Commentaire :** VS2Go vous offre une méthode sûre pour saisir votre mot de passe : le clavier virtuel. Cette option permet de protéger votre phrase secrète contre les enregistreurs de frappe qui pourraient être installés sur l'ordinateur que vous utilisez.

**Sixième étape. Cliquez** sur :  pour activer le *Clavier virtuel* :

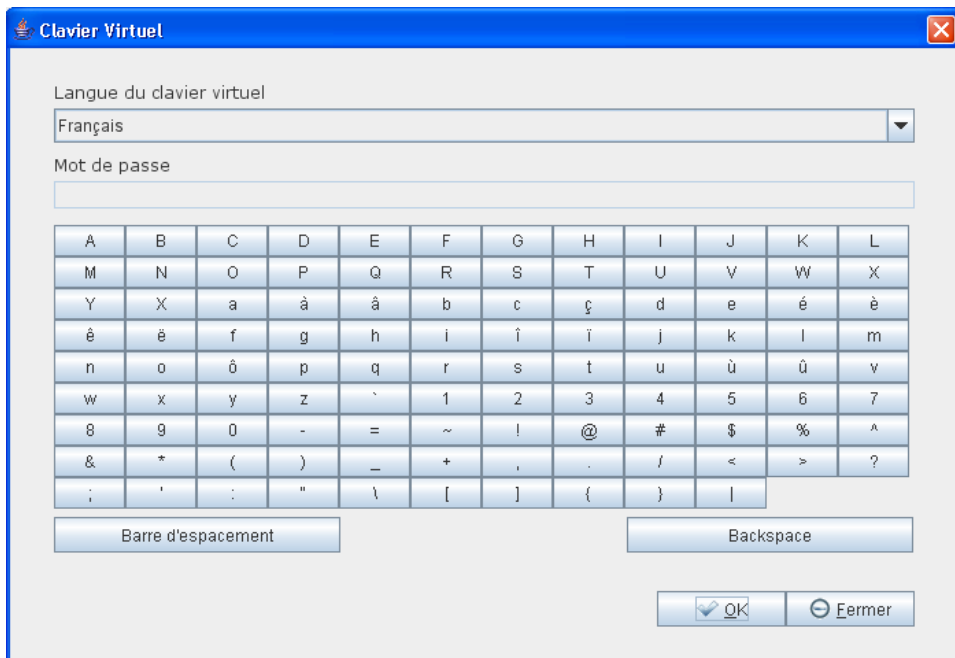



Figure 7 : Le clavier virtuel

**Septième étape.** Cliquez sur les touches correspondant à votre phrase secrète sur le *clavier virtuel*.

**Huitième étape.** Cliquez sur :  lorsque vous avez terminé.

**Neuvième étape.** Saisissez une seconde fois votre phrase secrète à l'aide du clavier virtuel. Les deux phrases doivent correspondre et doivent comprendre au moins 8 caractères. Lorsque tout concorde, le bouton  est activé et vous pouvez poursuivre le processus d'enregistrement.

La prochaine fenêtre présente le *contrat d'utilisation*.

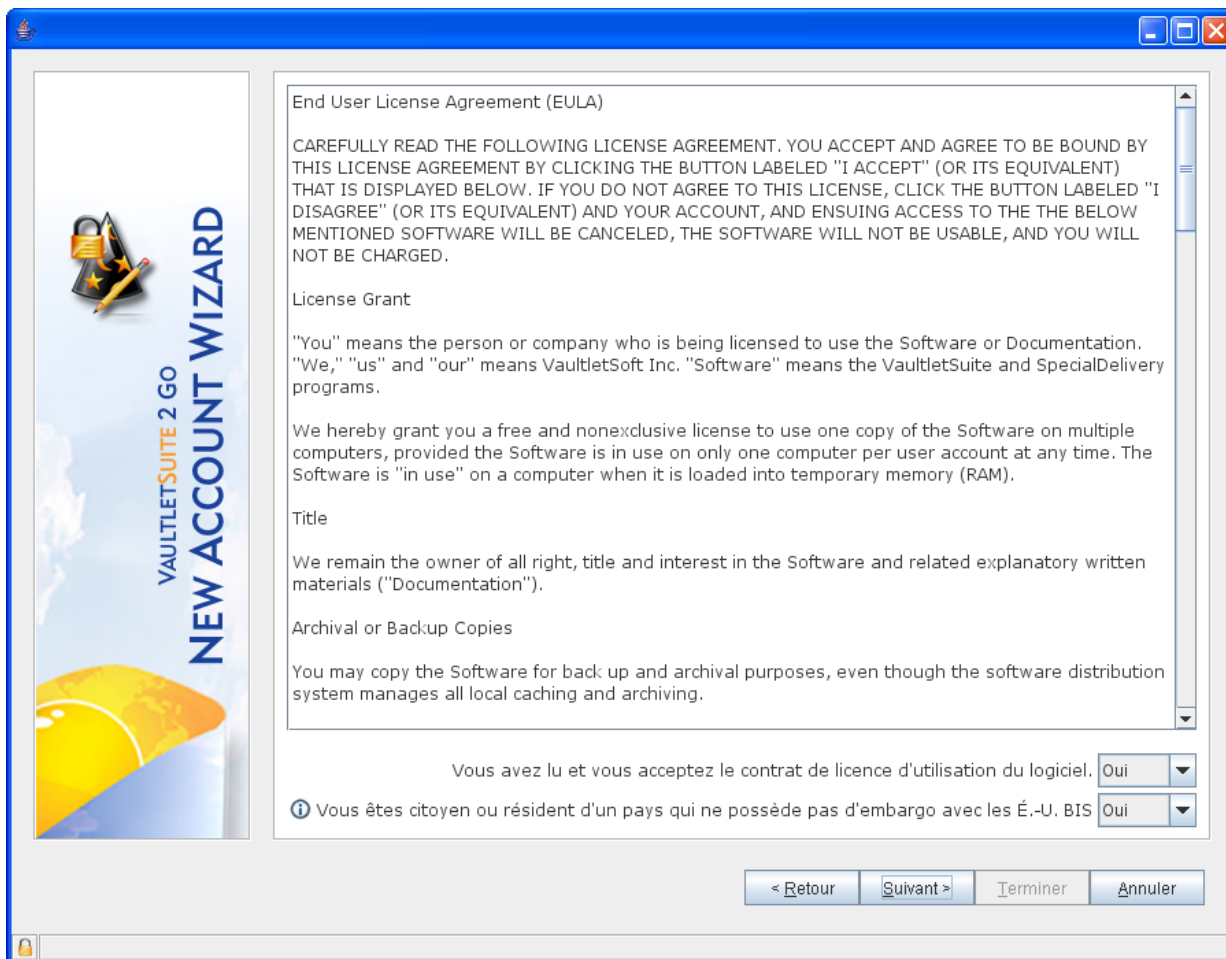


Figure 8 : La fenêtre du contrat d'utilisation

**Dixième étape.** Sélectionnez *Oui* dans les deux menus pour continuer.



La prochaine fenêtre présente les renseignements concernant les bénéficiaires et référents de VS2Go.

Nom : Terence Letesteur  
Adresse de courriel externe : tletesteur@riseup.net  
Compte VaultletSuite 2 Go : terence.letesteur  
Adresse du VaultletMail : terence.letesteur@vaultletsoft.com  
Type de compte : Inscription  
Préférences : Vous préférez la simplicité à la qualité de l'image.

📄 Groupe bénéficiaire : Front Line (www.frontlinedefenders.org) Dublin, Ireland  
📄 Adresse VaultletMail du référent :  
Période d'inscription : Spécial Blue Compte : Gratuit! pour une année  
Période d'inscription :

< Retour   Suivant >   Terminer   Annuler

Figure 9 : La fenêtre des bénéficiaires et référents

**Onzième étape.** Sélectionnez le groupe bénéficiaire auquel vous souhaitez que VaultletSoft? achemine ses dons et offre son soutien.

**Douzième étape.** Sélectionnez le compte *Special Blue* dans le menu *Période d'inscription*.

**Commentaire :** Ce type de compte vous donnera accès à la plupart des fonctions de VaultletSuite pour une période d'un an. Après onze mois, vous recevrez un courriel vous rappelant que votre période d'inscription d'un an tire à sa fin. Veuillez consulter la **Section 5. FAQ et questions récapitulatives** <sup>[165]</sup> pour plus de renseignements sur les moyens de prolonger votre période d'inscription.

**Treizième étape.** Cliquez sur :  pour activer la fenêtre suivante :

Nouveau compte, recherche de disque

📄 Avant de pouvoir commencer à utiliser VaultletSuite 2 Go, vous devez nous dire comment vous comptez l'utiliser sur cet ordinateur et si vous avez l'intention de transférer vos archives en passant d'un ordinateur à un autre.

Figure 10 : La fenêtre de recherche de disque pour un nouveau compte

**Quatorzième étape.** Cliquez sur le bouton *Fermer* pour activer la fenêtre de *recherche de disque*.

Vous devez maintenant choisir l'emplacement où les fichiers VS2Go seront stockés.

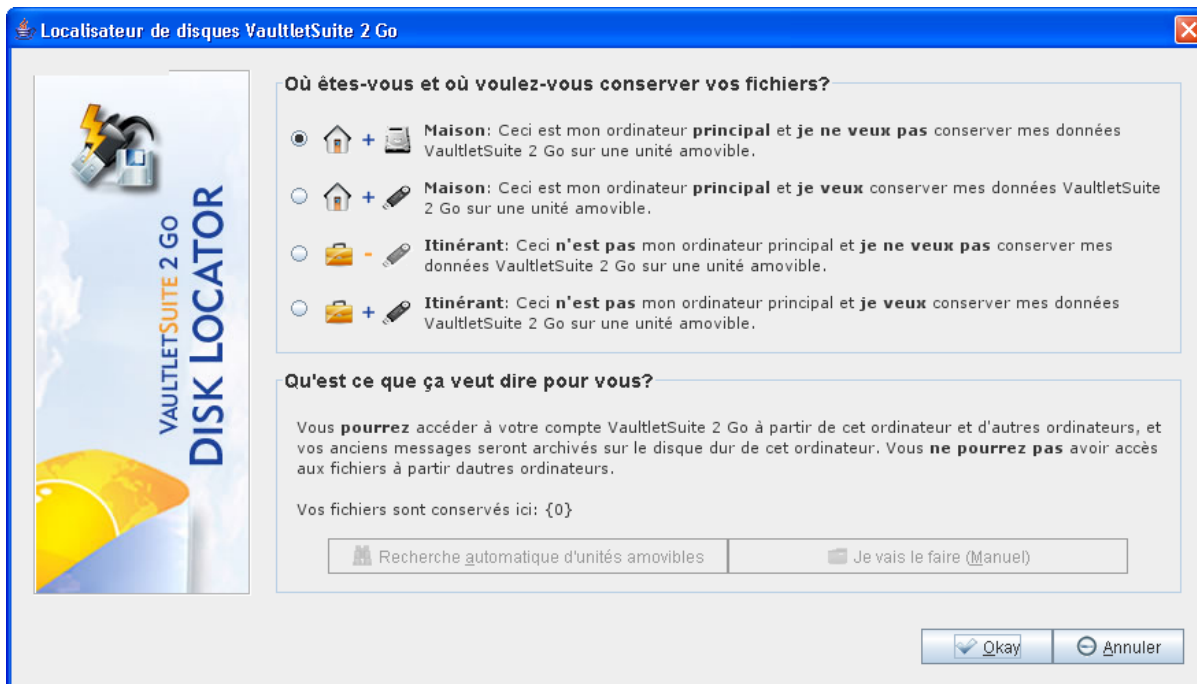


Figure 11 : La fenêtre Où êtes-vous et où voulez-vous conserver vos fichiers de VaultletSuite 2 Go

**Choisissez l'une des trois options de stockage de fichiers :**

Vous pouvez conserver les fichiers de votre compte VS2GO sur votre ordinateur, sur un serveur de Vaultlet ou sur une clé USB. Chacune des options est détaillée dans cette fenêtre, et vous pouvez lire de plus amples explications en **cochant** l'une ou l'autre. N'oubliez pas que si vous choisissez de conserver vos fichiers sur une clé USB, vous ne serez pas en mesure d'accéder à votre compte ou à vos archives à moins que vous ne transportiez la clé USB avec vous.

**Option 1** – Je désire sauvegarder tous mes fichiers et y accéder sur mon ordinateur seulement .

Comme le nom le suggère, vous ne pourrez accéder à votre compte qu'à partir de votre ordinateur.

**Première étape. Cochez** l'option *Maison : ceci est mon ordinateur principal et je ne veux pas conserver mes données VaultletSuite 2 Go sur une unité amovible.*

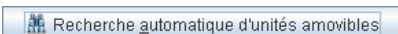
**Deuxième étape. Cliquez** sur :  pour continuer.

**Option 2** – Je désire conserver les données de mon compte et y accéder sur une clé USB

Si vous souhaitez accéder à VS2Go à partir de plusieurs ordinateurs différents (le logiciel VS2Go devra être installé sur chaque ordinateur utilisé), choisissez cette option et transportez les données du compte avec vous sur une clé USB.

**Première étape. Cochez** l'option 'Maison: ceci est mon ordinateur principal et je veux conserver mes données VaultletSuite 2 Go sur ma clé USB'.

Vous devrez alors indiquer à VS2Go où se trouve votre clé USB.

**Deuxième étape. Cliquez** sur : 

VS2Go effectuera une recherche sur votre ordinateur pour détecter des unités de stockage amovible. Si plus d'une unité sont trouvées, vous devrez en sélectionner une seule.

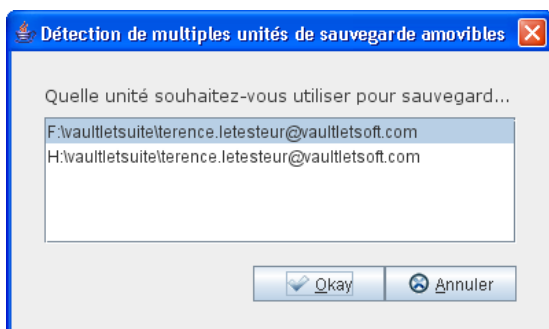


Figure 12 : La fenêtre Détection de multiples unités de stockage amovibles

Cette fenêtre devrait alors apparaître :

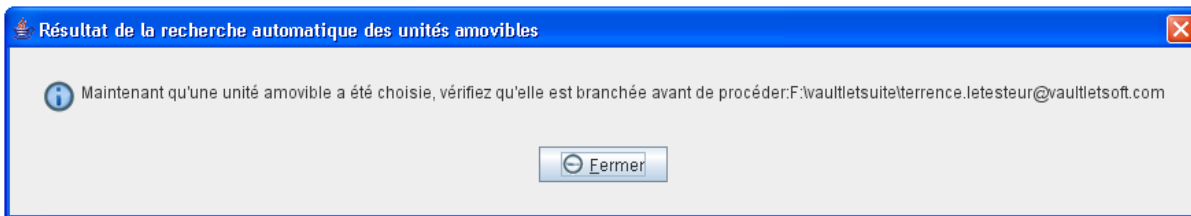


Figure 13 : La fenêtre Résultat de la recherche automatique des unités amovibles

La fenêtre de Détection d'unités amovibles affichera maintenant l'emplacement de votre clé USB, ainsi que le répertoire suggéré pour le stockage de vos données.

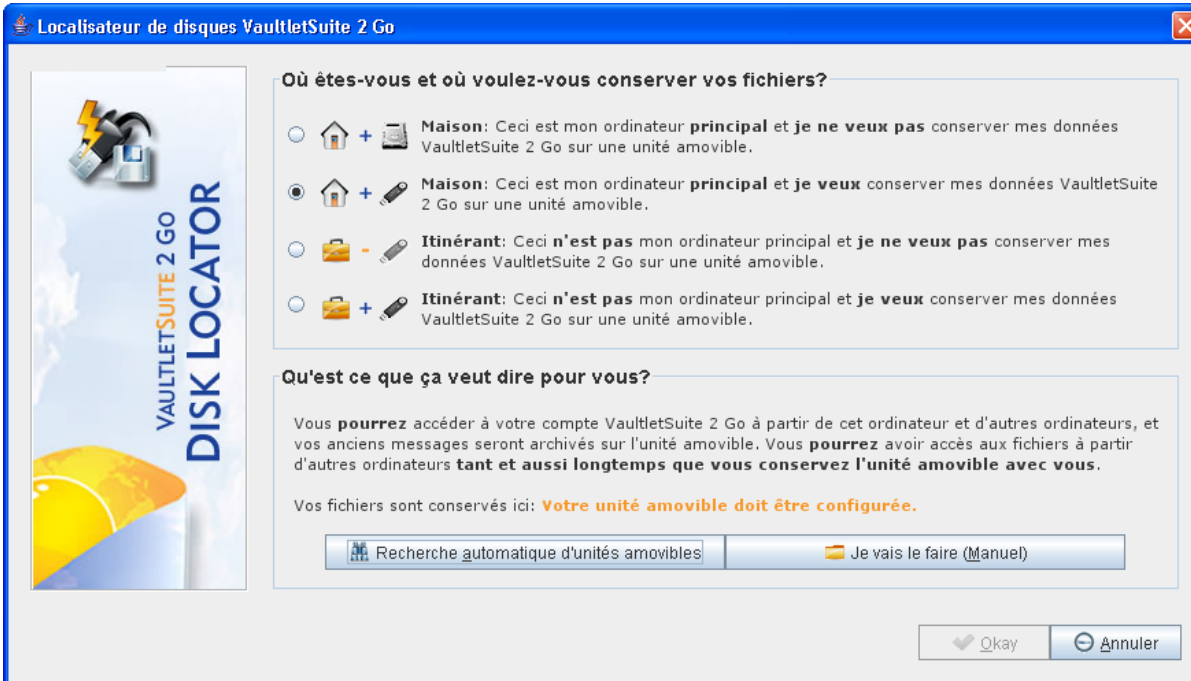


Figure 14 : La fenêtre Où êtes-vous et où voulez-vous conserver vos fichiers de VaultletSuite 2 Go

Si vous souhaitez changer le répertoire par défaut ou choisir une autre unité de stockage :

Troisième étape. Cliquez sur :  et sélectionnez l'emplacement désiré.

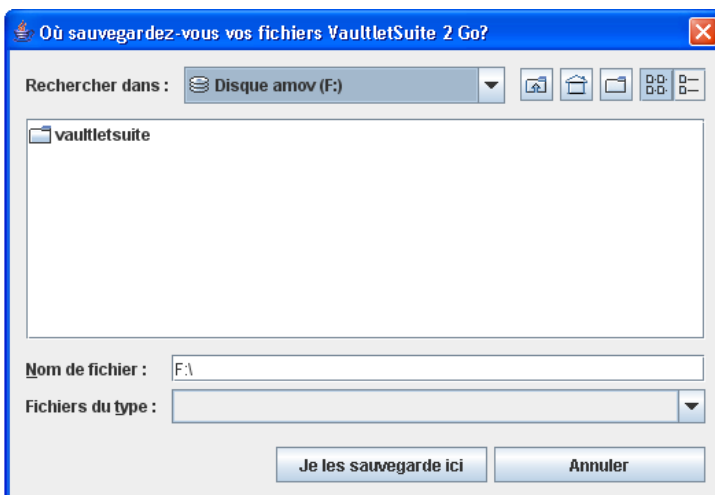
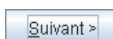


Figure 15 : La fenêtre Où sauvegardez-vous vos fichiers VaultletSuite 2 Go

Quatrième étape. Cliquez sur :  pour continuer.

**Commentaire :** Si vous choisissez de transporter les données du compte sur une clé USB, vous devrez la connecter à l'ordinateur avant de lancer le programme VS2Go. Vous devrez peut-être préciser son emplacement si vous vous êtes déjà connecté à partir d'autres ordinateurs.

**Option 3 – Je veux simplement recevoir et envoyer quelques nouveaux messages. Je n'ai pas besoin d'accéder à mes archives.**

**Première étape. Cochez l'option Itinérant:** Ceci n'est pas mon ordinateur principal et je ne veux pas conserver mes données VaultletSuite 2 Go sur une unité amovible.

Deuxième étape. Cliquez sur : 

### Finaliser l'enregistrement de votre compte VS2Go

Finalement, une fenêtre vous présente une vue d'ensemble de votre nouveau compte Vaultletsoft. Assurez-vous que tous les renseignements sont corrects.

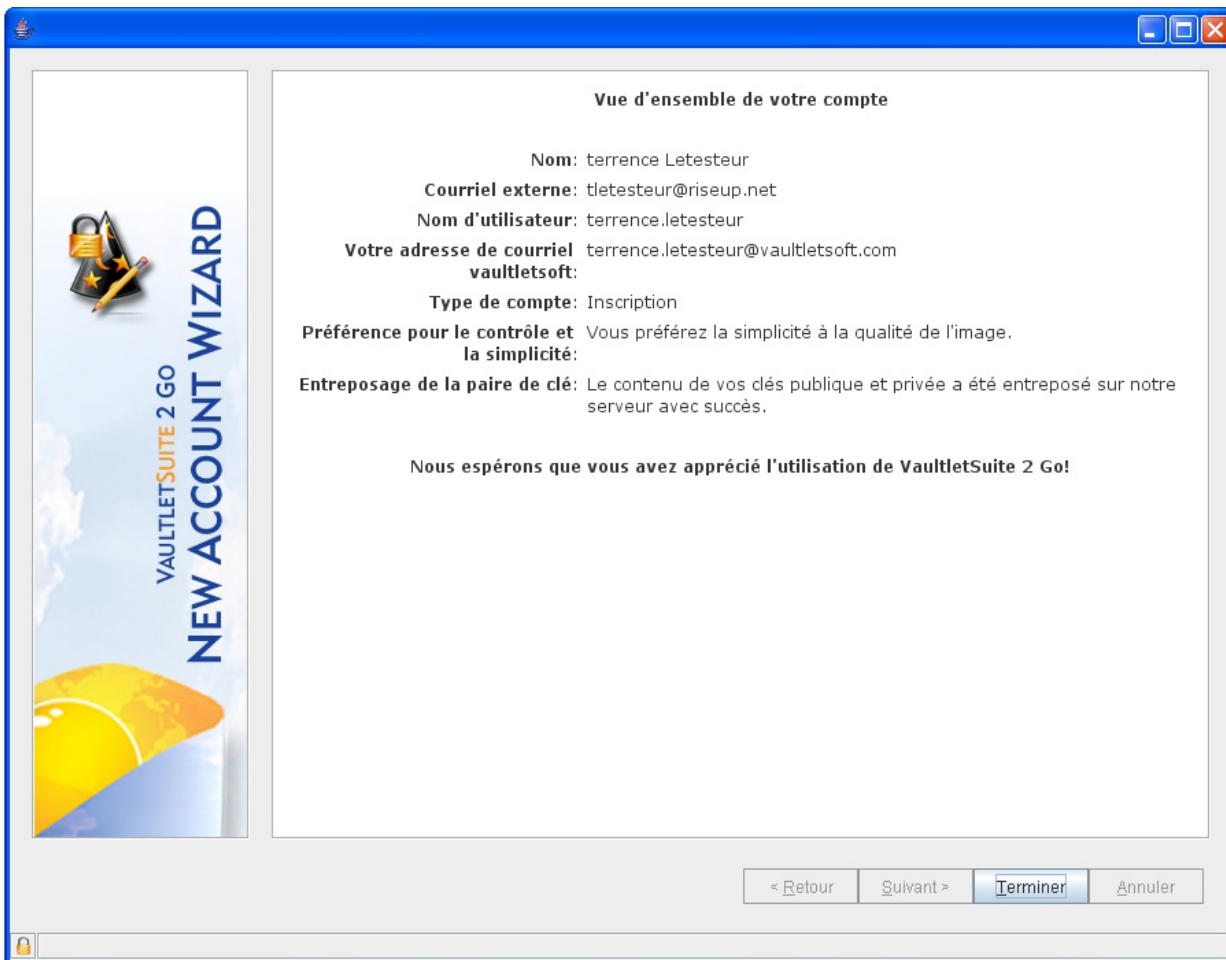




Figure 16 : Nouveau compte VaultletSuite 2 Go

Première étape. Cliquez sur :  pour finaliser la procédure de création du compte.

Félicitations, vous venez d'enregistrer un compte de courrier électronique VS2Go. Il est possible qu'une fenêtre apparaisse à ce moment pour vous présenter un *Message Système VS2Go* décrivant quelques-unes des nouvelles fonctions du logiciel. Cliquez sur :  pour continuer. Il est conseillé d'installer toutes les mises à jour proposées.

### 2.3 Sur l'actualisation de VS2Go

Lorsque vous lancez VS2Go, il est possible que l'on vous demande d'actualiser le logiciel avec la plus récente mise à jour de VS2Go. Les mises à jour mineures sont optionnelles mais les mises à jour majeures du programme doivent être installées avant que vous puissiez continuer à vous servir du programme. Ces mises à jour comprennent d'importantes corrections de sécurité et autres améliorations.

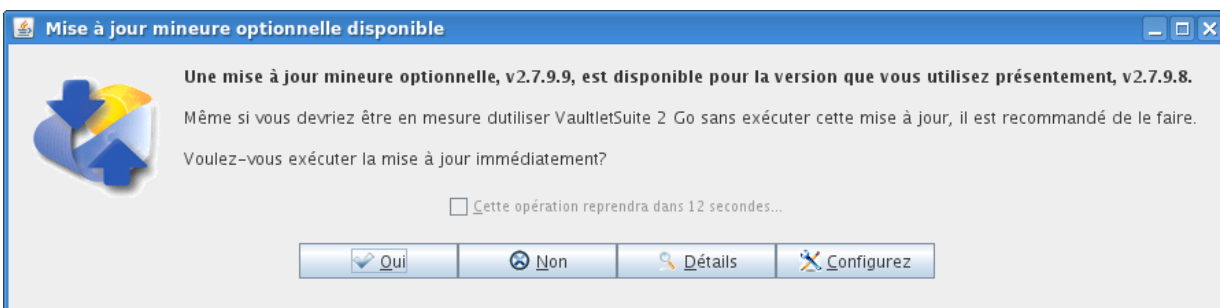


Figure 17 : La fenêtre d'alerte de mises à jours mineures optionnelles

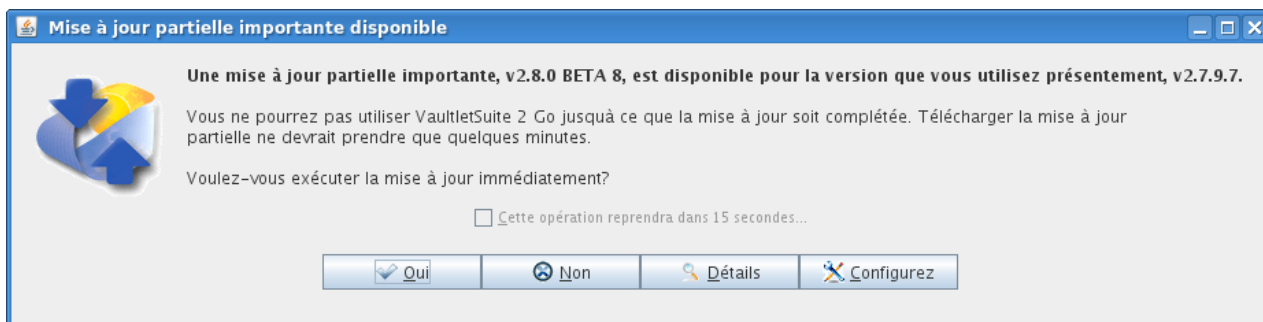


Figure 18 : La fenêtre d'alerte de mises à jours majeures partielles

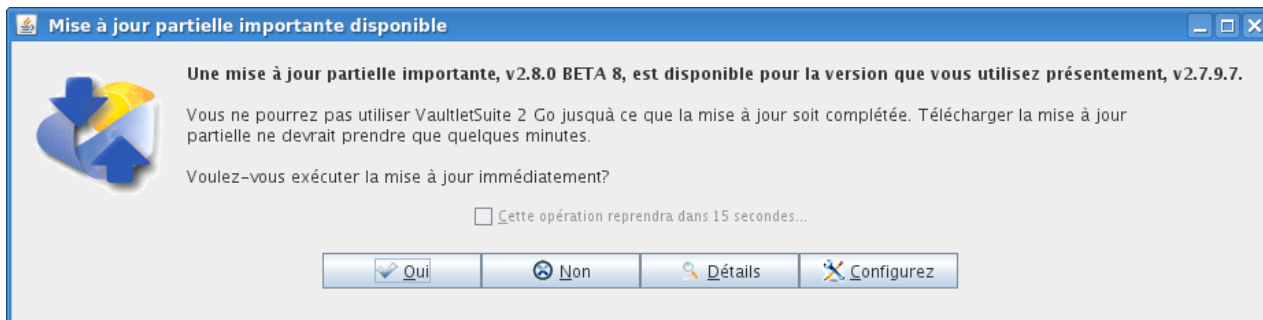


Figure 19: La fenêtre d'alerte de mise à jour majeure partielle supplémentaire

Les mises à jour seront automatiquement téléchargées et installées sur votre ordinateur ou votre unité de stockage amovible.

## Comment utiliser VS2Go

Maintenant que vous avez enregistré un compte, vous pouvez commencer à utiliser l'un des systèmes de courrier électronique les plus sûrs disponibles sur Internet actuellement! Après l'enregistrement (ou après vous être dûment connecté), vous serez dirigé vers l'interface de gestion du courriel.


**Première étape.** Cliquez sur :  ou sélectionnez : Démarrer > Programmes > VaultletSuite2Go > VaultletSuite2Go pour activer la console principale de VaultletSuite 2 Go et la fenêtre de connexion.



Figure 20 : La fenêtre Bienvenue à VaultletSuite 2 Go! [@vaultletsoft.com]

**Commentaire :** Si vous avez changé d'ordinateur depuis la dernière fois que vous avez accédé à votre compte, VS2Go vous interrogera sur l'emplacement de vos archives et de vos données VaultSoft. Les premières fois que vous vous connecterez, une fenêtre s'activera pour vous informer des nouvelles fonctions de VS2Go.

La fenêtre de la corbeille d'arrivée de VaultletMail apparaîtra alors.

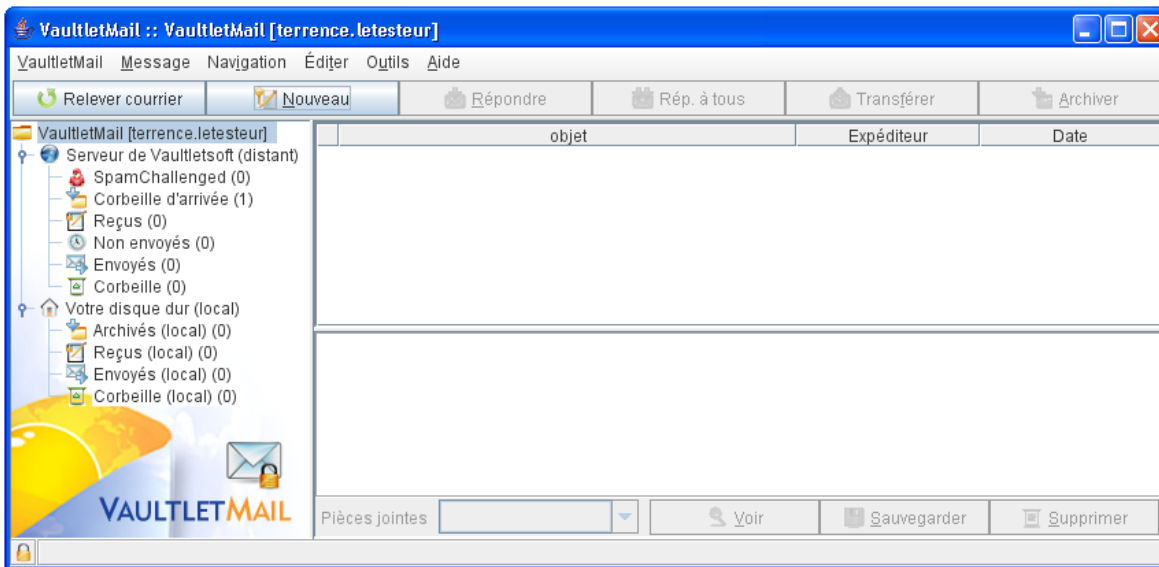


Figure 21 : La fenêtre de la corbeille d'arrivée de VaultletSuite 2

Remarquez que la console principale de VaultletSuite 2 Go, qui vous permet de naviguer entre le programme de courriel, l'outil de stockage de fichiers et l'outil de gestion de mots de passe de VaultletSuite, est toujours activée.

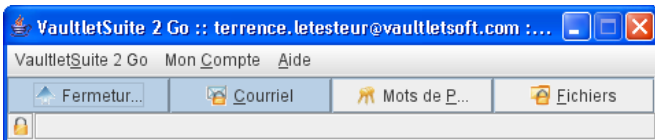


Figure 22 : La console principale de VaultletSuite 2 Go

### 3.1 Comment utiliser les fonctions principales de VS2Go

En fait, VS2Go fonctionne comme n'importe quel autre client de messagerie. Vous rédigez un message, choisissez des destinataires et leur envoyez le message. Cependant, VS2Go offre un éventail de fonctions de sécurité avancées que la plupart des autres programmes de courriel n'ont pas. Dans cette section, vous apprendrez à rédiger des messages et à gérer vos archives de courriel et vos fichiers.

**Pour rédiger un nouveau message :**

**Première étape.** Cliquez sur :  pour ouvrir une fenêtre de *Nouveau message*.

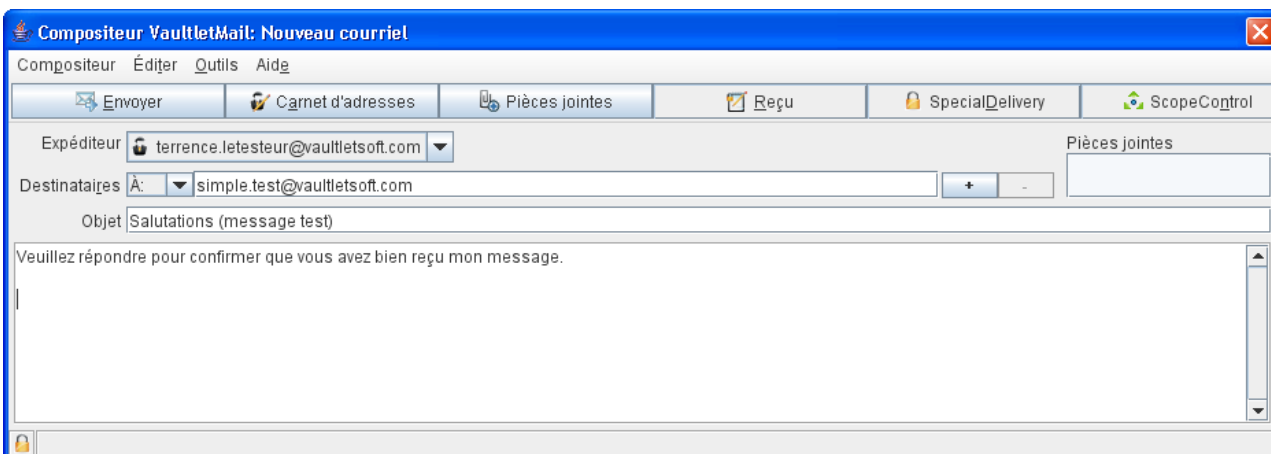



Figure 23. La fenêtre VaultletMail: nouveau message

**Commentaire :** Il est conseillé d'agrandir la fenêtre de *Rédaction* afin d'afficher toutes les fonctions du menu.

**Deuxième étape. Rédigez** votre message, saisissez l'adresse du destinataire et **cliquez** sur :  lorsque vous avez terminé.

VaultletMail chiffrera automatiquement tous les messages envoyés à d'autres destinataires VS2Go (qui disposent d'une adresse @vaultletsoft.com). La prochaine section donne des directives concernant le chiffrement de messages envoyés à des destinataires qui n'ont pas de compte VaultletSoft.

**Pour transférer des messages dans l'archive :**

La liste des dossiers qui se trouve à gauche de la fenêtre principale de votre *corbeille d'arrivée* est divisée en trois catégories : *Serveur de Vaultletsoft (distant)* et *Votre disque dur (local)*, tel qu'illustré à la Figure 21. Tous les nouveaux messages, envoyés et reçus, sont initialement conservés sur un serveur de Vaultletsoft. Ce dernier offre un espace limité

et un temps limité de stockage. Effectuez régulièrement le transfert de vos messages vers votre ordinateur ou votre dispositif de stockage amovible (là où vous avez choisi de stocker vos archives à la section 2, ci-dessus). Votre compte local peut être aussi volumineux que votre ordinateur ou votre dispositif de stockage le permet. Tous vos messages seront stockés par l'entremise du chiffrement sécurisé VS2Go.

**Première étape. Sélectionnez** le(s) message(s) que vous souhaitez archiver.

**Deuxième étape. Sélectionnez : Message > Archiver** dans la barre de menus.

N'oubliez pas que si vous avez choisi l'option *Itinérant* pour transporter vos archives avec vous sur un dispositif amovible, vous devrez avoir ce dispositif avec vous en tout temps pour accéder à vos messages archivés. Vous pouvez toutefois recevoir et rédiger de nouveaux messages sans passer par votre dispositif amovible.

### 3.2 Comment utiliser VaultletFiler

VS2Go offre un service sécurisé de stockage de fichiers et utilise l'archive (que vous avez créé sur votre ordinateur ou sur votre clé USB) à cette fin. Vous pouvez transférer plusieurs fichiers que vous souhaitez protéger à l'aide du chiffrement VS2Go, et y accéder à partir de votre ordinateur ou dispositif de stockage amovible. Gardez à l'esprit que les fichiers qui se trouvent sur votre ordinateur seront transférés et chiffrés par VS2Go. Vous ne pourrez y accéder que si vous êtes connecté à Internet et à votre compte (les prochaines versions de Vaultletsoft intégreront une fonction d'accès hors ligne). Le VaultletFiler est accessible par la console principale de VaultletSuite 2 Go.

**Première étape. Sélectionnez : VaultletSuite 2 Go > VaultletFiler** pour ouvrir la fenêtre *VaultletFiler*

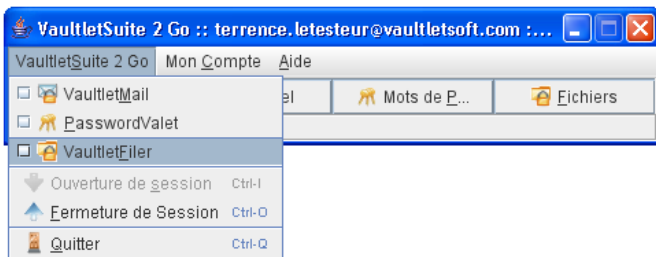


Figure 24. Sélectionner VaultletFiler par la console principale de VaultletSuite 2 Go

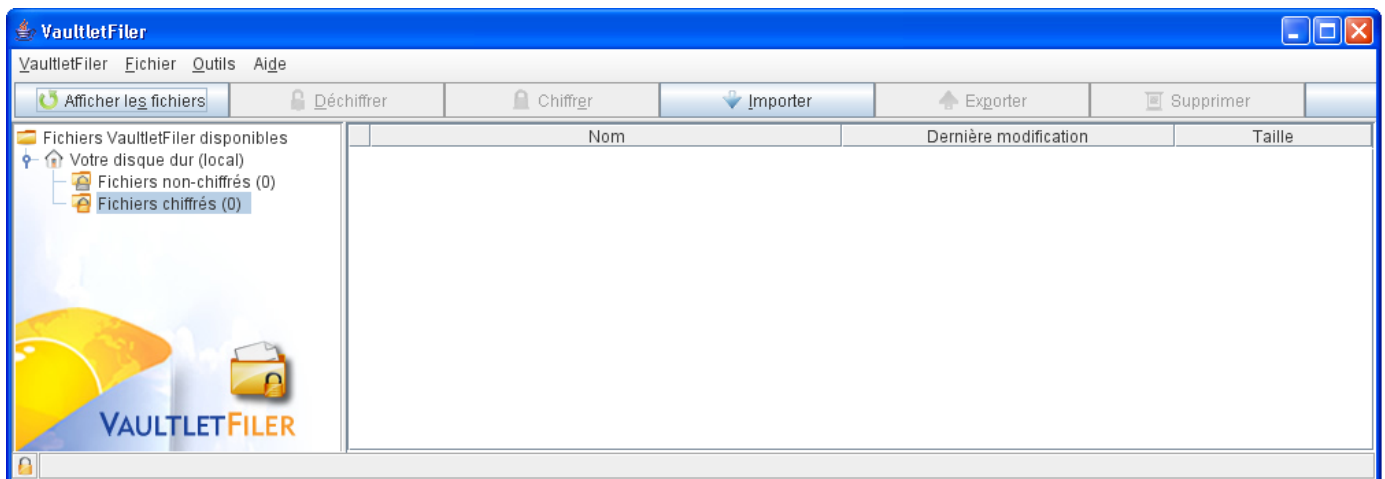


Figure 25. La fenêtre VaultletFiler

Pour importer (ou transférer) des documents dans le *VaultletFiler*?, suivez les étapes énumérées ci-dessous :

**Deuxième étape. Cliquez** sur : 

**Troisième étape. Sélectionnez** le(s) fichier(s) à importer.

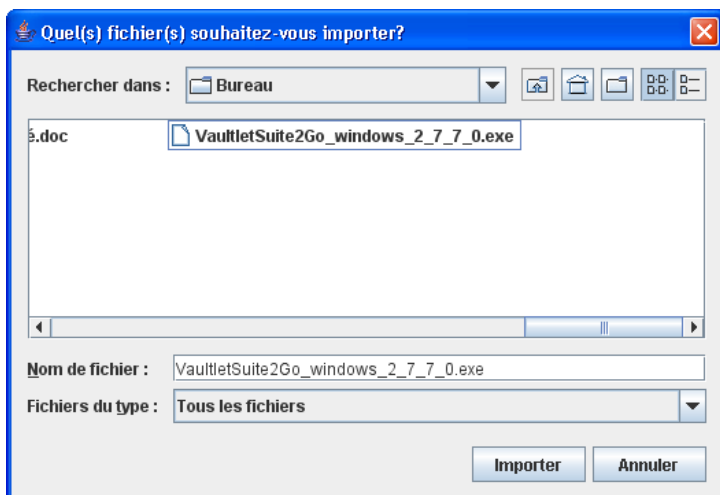


Figure 26. La fenêtre Quel(s) fichier(s) souhaitez-vous importer?

**Quatrième étape. Cliquez sur :** *Importer*

Le fichier apparaît maintenant dans la fenêtre *Fichiers chiffrés* :

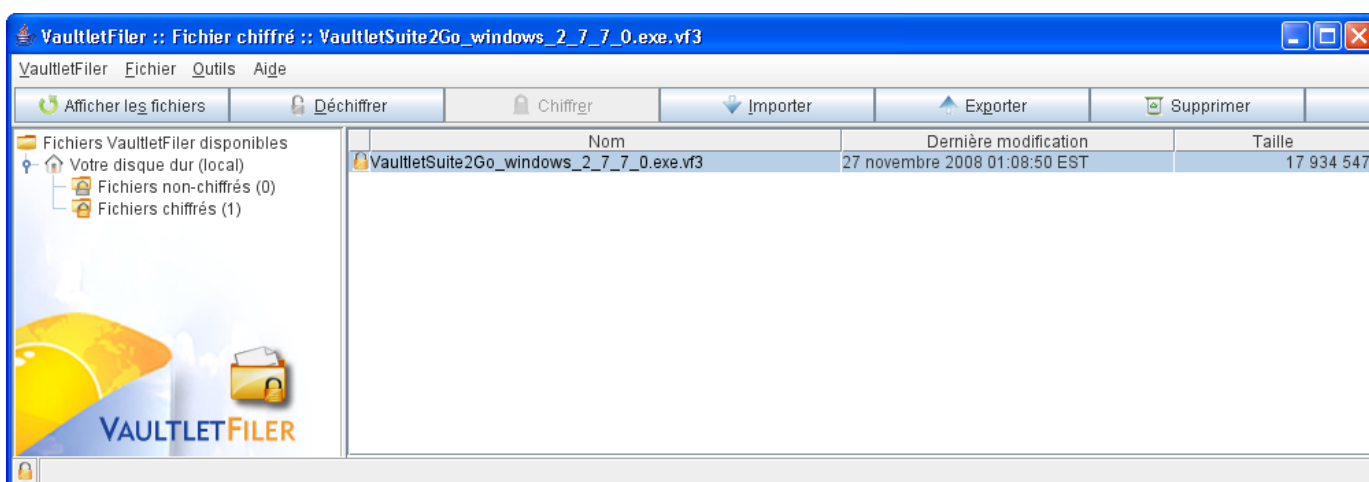


Figure 27. Les fichiers chiffrés affichés dans le VaultletFiler

Pour accéder à ce(s) fichier(s) ultérieurement, vous devrez d'abord le(s) exporter et le(s) déchiffrer. Pour ce faire, suivez les étapes énumérées ci-dessous :

**Première étape. Sélectionnez** le fichier à exporter dans la fenêtre *Fichiers chiffrés*.

**Deuxième étape. Cliquez sur :**

**Troisième étape. Choisissez** l'emplacement où les fichiers doivent être exportés.

On vous demandera alors si vous souhaitez d'abord déchiffrer le fichier. Si vous voulez y accéder (c.-à-d. le modifier ou l'activer), vous devrez déchiffrer le fichier.

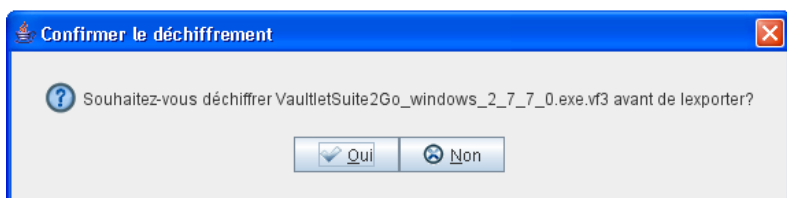


Figure 28: La Fenêtre Confirmer le déchiffrement

**Quatrième étape. Cliquez sur** *Oui* pour déchiffrer et exporter le(s) fichier(s) sélectionné(s) vers l'emplacement souhaité.

## Fonctions avancées VaultletMail


VS2Go comporte quelques fonctions supplémentaires qui augmentent encore le niveau de sécurité de vos communications par courrier électronique. Vous devez avoir choisi un *Compte bleu* lors de l'enregistrement pour profiter pleinement de ces fonctions.

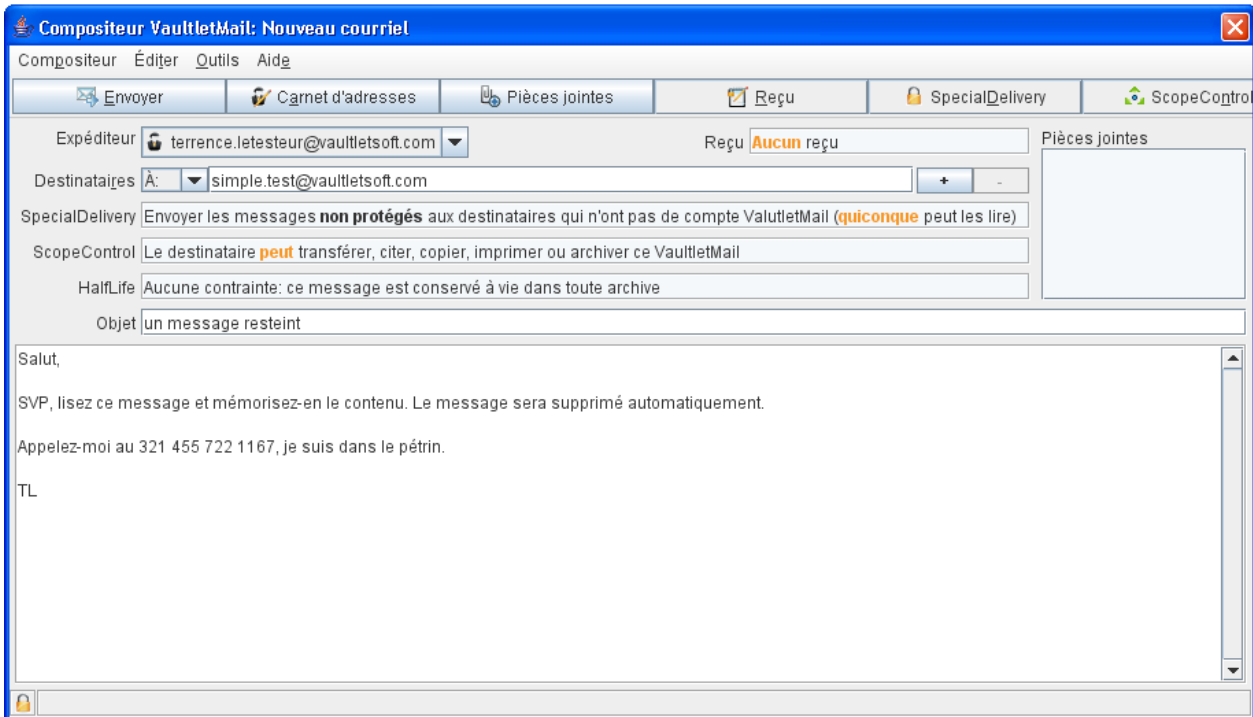
- **Half-Life** – Vous permet de déterminer la durée de vie d'un message à partir du moment où le destinataire l'a ouvert. Vous pouvez préciser d'avance le nombre de fois que le message pourra être lu, ou déterminer une limite de temps avant que le message ne soit automatiquement supprimé. Cette fonction est utile pour envoyer des renseignements



sensibles qui ne doivent plus être accessibles après une période de temps donnée.

- **ScopeControl** – Vous permet de restreindre la capacité de votre destinataire à transférer votre message à une tierce partie ou de copier le contenu affiché dans la fenêtre principale du message original. Cela est utile pour empêcher qu'un destinataire commette accidentellement une 'fuite' des renseignements qui se trouvent dans votre message.
- **SpecialDelivery** – Vous permet d'envoyer des messages chiffrés, et d'utiliser les fonctions *Half-Life* et *ScopeControl* si nécessaire, à l'extérieur du domaine VaultletSoft. Cela signifie que vous pouvez maintenir votre confidentialité lorsque vous communiquez avec des personnes qui utilisent d'autres services de messagerie (même des services non sécurisés).

Pour vérifier si ces fonctions complémentaires sont activées, **cliquez** sur :  dans la fenêtre de *Rédaction de message VaultletMail*.



**Commentaire** : Il est possible que vous deviez étirer la fenêtre pour afficher cet icône.

#### 4.1 La fonction Half-Life

Il est possible de limiter la durée de vie d'un message, à partir du moment que ce dernier est arrivé dans la corbeille d'arrivée du destinataire. Pour ce faire, il suffit de **cliquer** sur le bouton *HalfLife* dans la barre de menus de la fenêtre de rédaction de message de *VaultletMail*.

**Première étape.** Cliquez sur :  pour activer la fonction *Half-Life*.

**Deuxième étape.** Sélectionnez la durée de vie souhaitée pour le message (c.-à-d. la limite de temps que le message sera affiché avant d'être automatiquement supprimé, ou le nombre limite de fois que le message peut être ouvert, ou une combinaison des deux).

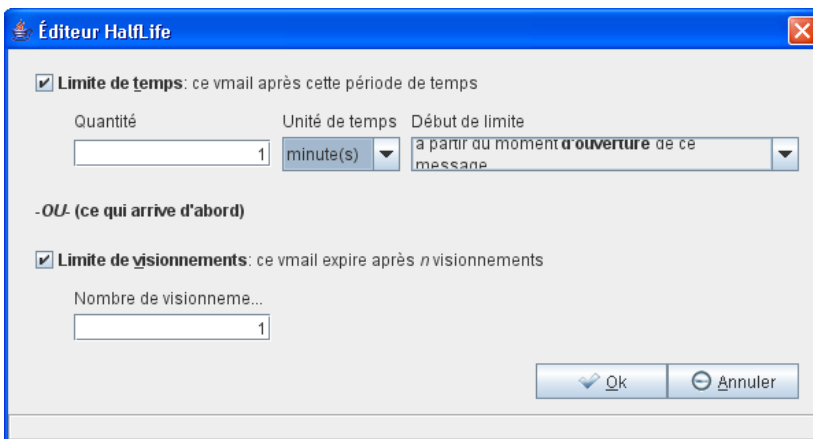
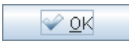


Figure 29. La fenêtre de la fonction *HalfLife*

**Troisième étape.** Cliquez sur :  lorsque vos réglages sont terminés.

**Commentaire** : La description de la fonction *HalfLife*, au dessus de votre message, devrait maintenant tenir compte des nouveaux réglages.

HalfLife [Ne peut être lu que 1 minute(s) à partir du moment d'ouverture du message --ou-- ne peut être vu plus de 1 foi(s)]

Figure 30 : La description de la fonction HalfLife

Quatrième étape. Rédigez votre message et cliquez sur : 

Le destinataire recevra alors votre message. Il pourra voir les restrictions que vous avez imposées, tel qu'illustré ci-dessous :

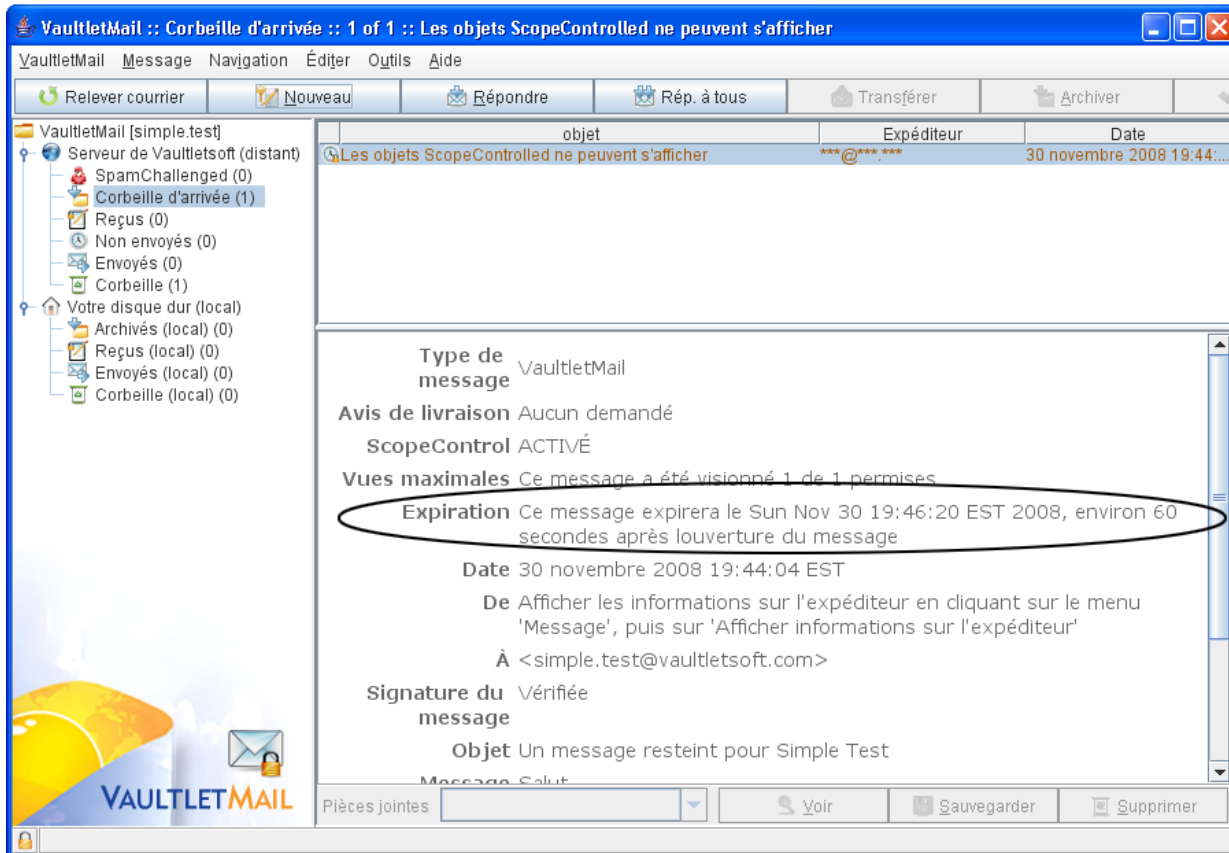


Figure 31. La corbeille d'arrivée VaultletMail de votre destinataire affichant le message que vous avez envoyé et sa durée de vie

Quand la durée de vie du message sera révolue, ou quand la limite du nombre de fois où le message peut être affiché sera atteinte, le message sera automatiquement supprimé.

## 4.2 La fonction Scope Control

Vous pouvez empêcher vos destinataires de transférer votre message à une tierce partie ou de copier le contenu de votre message. Cela peut s'avérer utile pour empêcher que des 'accidents' se produisent et que votre message circule sur des listes électroniques.

Première étape. Cliquez sur :  dans la fenêtre de rédaction de message VaultletMail.

Remarquez que la description de la fonction Scope Control, au dessus de votre message, est maintenant quelque peu modifiée :

ScopeControl [Le destinataire ne peut pas transférer, citer, copier, imprimer ou archiver ce VaultletMail]

Figure 32 : La description de la fonction Scope Control

Il est maintenant impossible à vos destinataires de transférer votre message ou d'en copier, archiver ou imprimer le contenu.

## 4.3 La fonction SpecialDelivery

La fonction SpecialDelivery apporte la sécurité et la fonctionnalité de VS2Go à tous les utilisateurs de courrier électronique. Elle permet d'envoyer des messages chiffrés à n'importe quelle adresse de courriel (et d'utiliser HalfLife? et Scope Control si nécessaire). Cela peut paraître une tâche impossible, mais le truc est simple : il s'agit d'envoyer le message chiffré et d'inclure un lien vers un visualiseur sécurisé de SpecialDelivery, situé sur le site Internet de VaultletSoft?, qui permet d'afficher le message de façon sécurisée.

**Commentaire :** Initialement, cette approche peut sembler laborieuse à vos correspondants. Par contre, lorsque ceux-ci auront complété le processus une première fois, tous les échanges subséquents seront considérablement plus rapides. Vous devez vous rappeler que si vous et vos correspondants voulez éviter que ces derniers soient en danger en utilisant un service de courriel non sécurisé, alors il est judicieux de prendre cette mesure de sécurité supplémentaire.

Première étape. Cliquez sur :  après avoir saisi une adresse de courriel externe dans le champ

Destinataires: Remarquez que la description de la fonction *Special Delivery*, au dessus de votre message, est maintenant quelque peu modifiée :

SpecialDelivery **Protéger** les messages **avant** de les envoyer aux destinataires qui n'ont pas de compte VaultletMail

Figure 33 : La description de la fonction *Special Delivery*

Vous pouvez maintenant activer les fonctions *HalfLife* et *Scope Control*, si nécessaire.

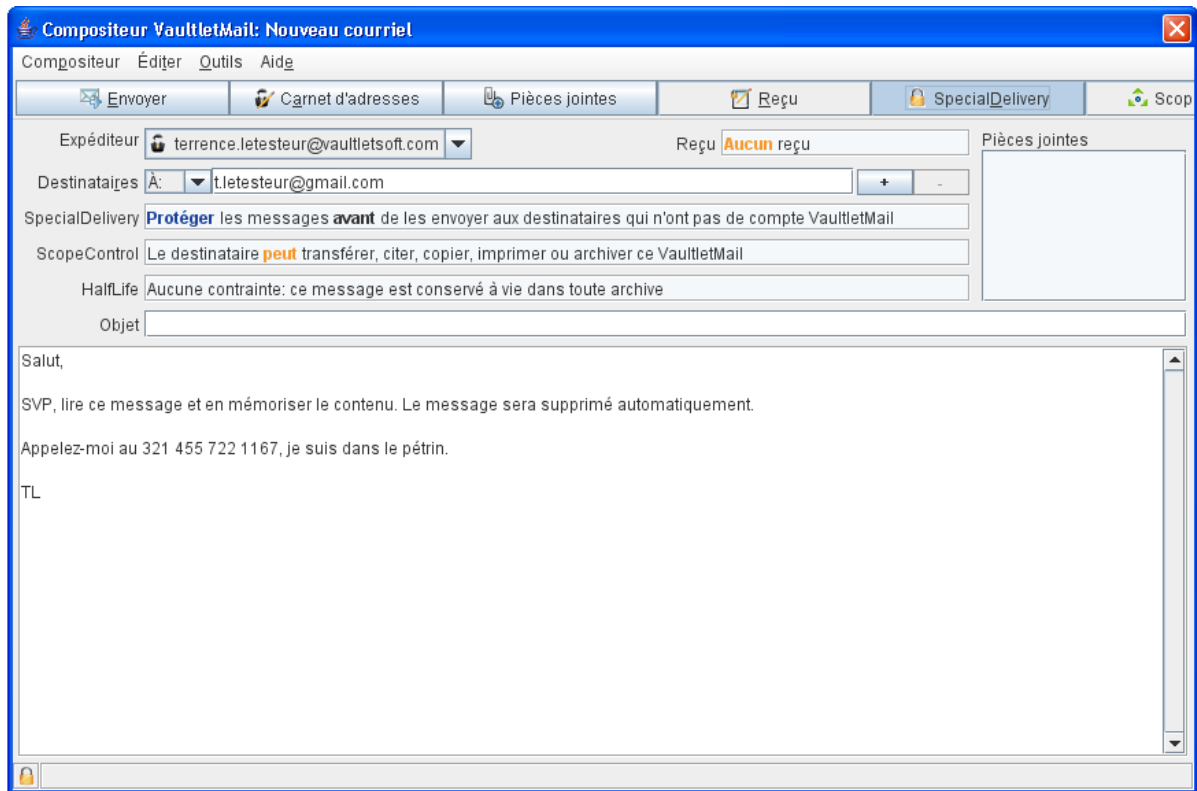



Figure 34: La fenêtre de rédaction de nouveau message VaultletMail

**Deuxième étape. Rédigez votre message et envoyez-le.**

On vous demandera de créer un code secret, que votre destinataire devra **saisir à l'identique** lorsque cela lui sera demandé par le système VS2Go. Cette opération sert à authentifier l'identité des deux parties en communication.

**Troisième étape. Saisissez un code secret (d'au moins 8 caractères) et cliquez sur :** 

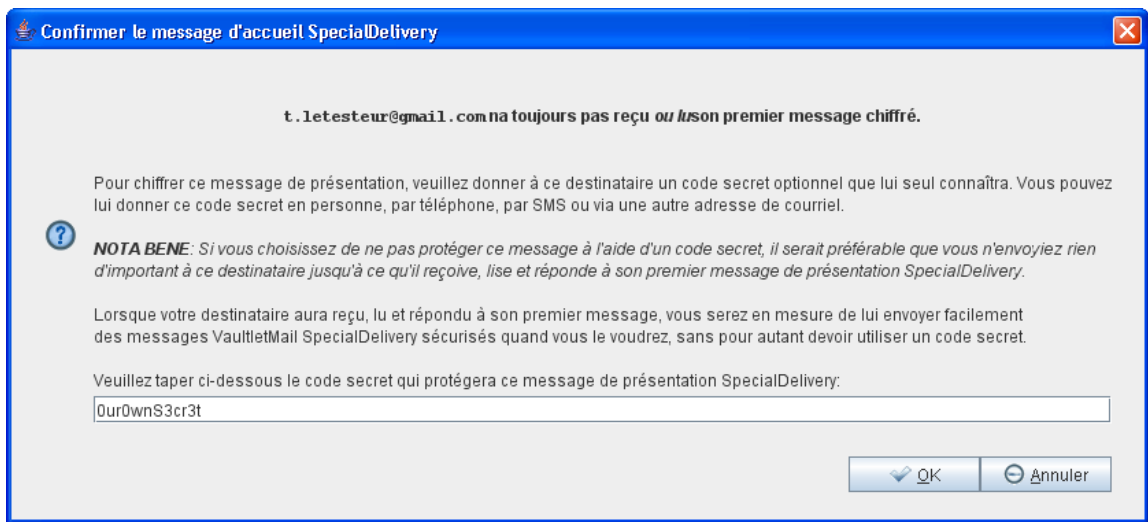


Figure 35 : La fenêtre Confirmer le message d'accueil SpecialDelivery

Passer le code secret à votre correspondant par SMS, en personne ou par téléphone. N'oubliez pas que cette opération d'authentification ne doit être effectuée qu'une seule fois pour chaque nouveau destinataire.

**Directives à l'intention du destinataire**

Vous recevrez le message VaultletSoft dans votre programme de messagerie normal.

**Objet:** VaultletMail SpecialDelivery: un message restreint  
**De:** "terrence Letesteur" <terrence.letesteur@vaultletsoft.com>  
**Date:** Dim 30 novembre 2008 19:31  
**À:** tletesteur@riseup.net  
**Priorité :** Normale  
**Options:** [Afficher l'en-tête complet](#) | [Voir la version imprimante](#) | [Télécharger en tant que fichier](#) | [Ajout](#)

Hi,

I'm sending you a secret and secure VaultletMail SpecialDelivery message that nobody else can read.

To read the secure contents of this secret message, hit "Ctrl + A" (select all) on your keyboard, followed by "Ctrl + C" (copy).

Once you've done that, click on this link to view it:  
<https://www.vaultletsoft.com/start/specialdelivery-applet.html>

Best,

terrence

--

p.s.: To find out more about VaultletMail SpecialDelivery messages, go here:  
<https://www.vaultletsoft.com/products/specialdelivery.html>

Figure 36 : Un message SpecialDelivery de VaultletSoft

**Première étape.** Suivez les directives incluses dans le message, en **copiant** le contenu au complet. **Cliquez** sur le lien pour ouvrir un nouvelle fenêtre de navigateur.

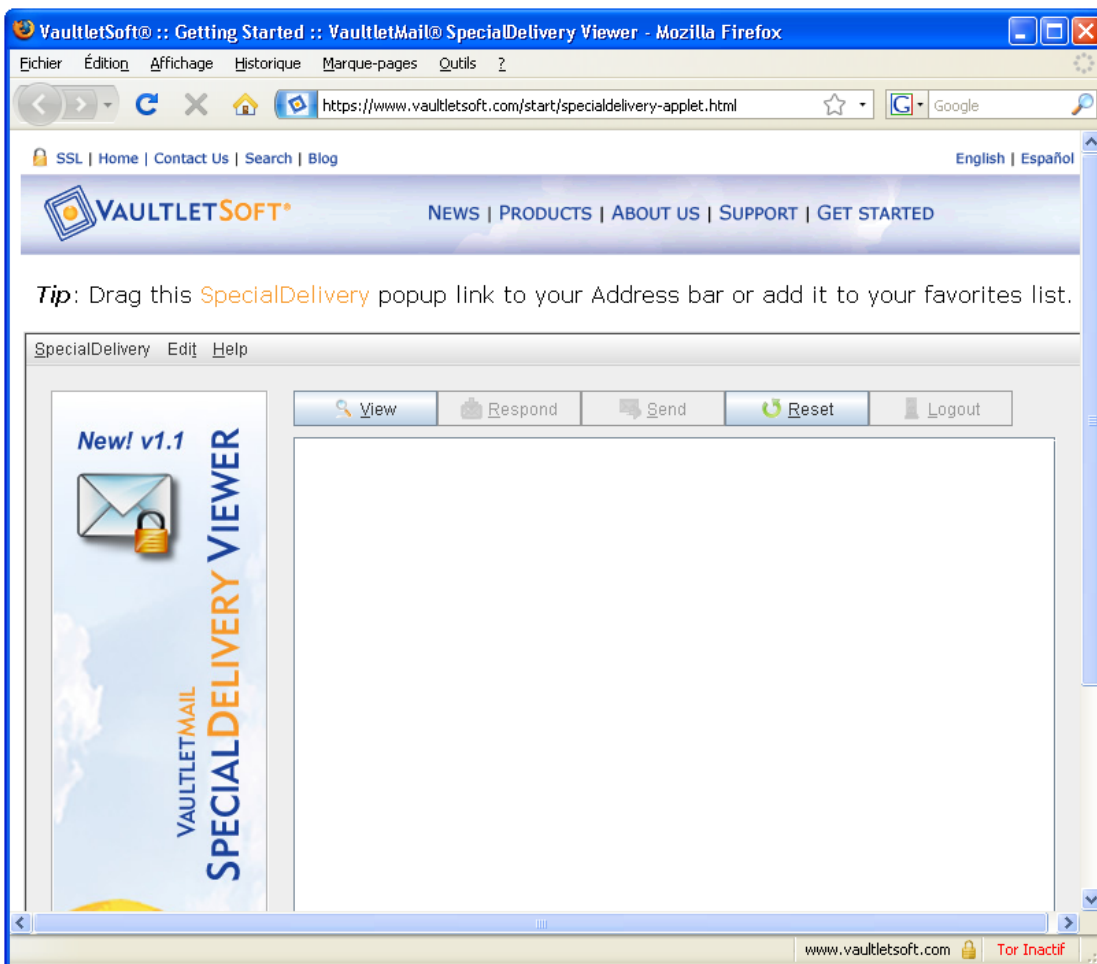


Figure 37. Le message SpecialDelivery de VaultletSoft Message affiché dans un compte de courriel non-VaultletSoft

Lorsque la page sera chargée, on vous demandera d'installer l'application Java depuis le site de VaultletSoft Inc. Il s'agit d'un petit programme qui effectuera le chiffrement et le déchiffrement des messages VaultletSoft sur votre ordinateur. Il est possible que l'on vous demande si vous souhaitez 'Toujours faire confiance à cet éditeur'. Prenez votre décision en fonction de si vous voulez ou non répondre à cette question chaque fois que vous lancez le visualiseur SpecialDelivery.

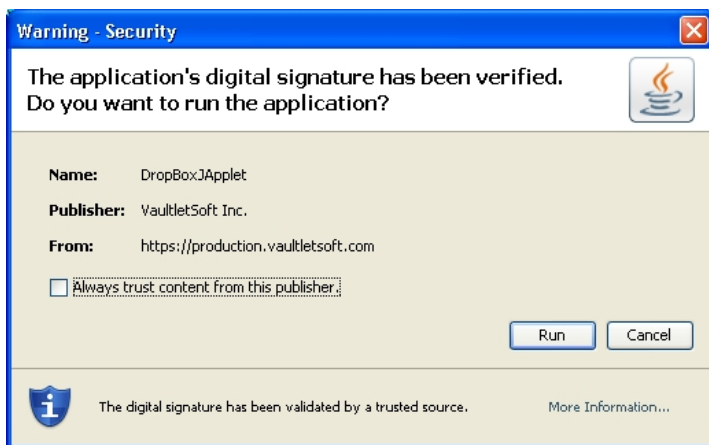


Figure 38 : La fenêtre d'alerte de sécurité

Deuxième étape. Cliquez sur **Run**.

Lorsque l'installation est terminée, faites **Ctrl+V** pour coller le contenu du courriel dans la fenêtre appropriée (si cela ne s'est pas produit automatiquement).

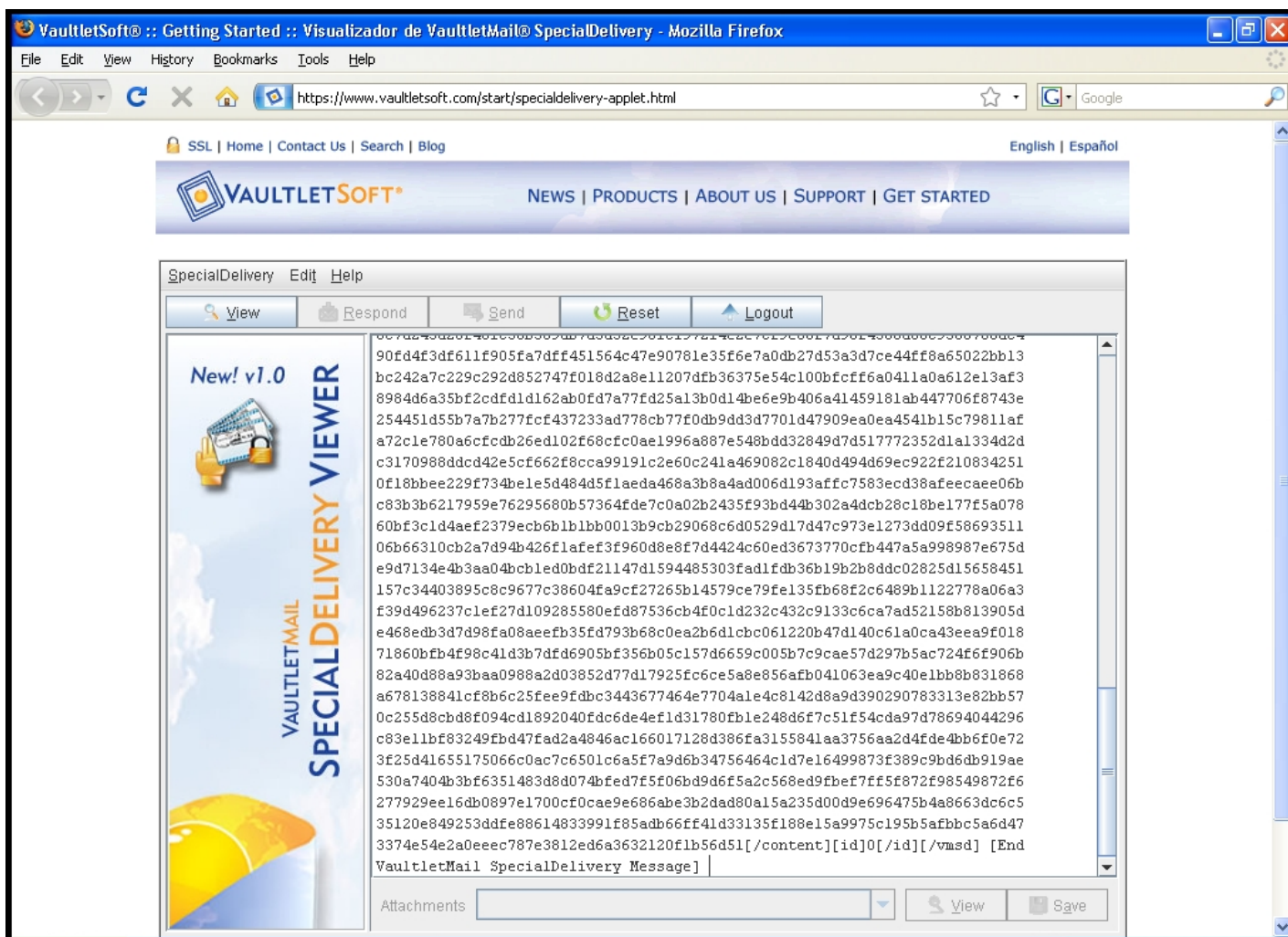


Figure 39 : La fenêtre Getting Started de VaultletSoft

Troisième étape. Cliquez sur :  pour le déchiffrer.

Le système commencera à déchiffrer le message. On vous demandera de créer un compte VS2Go, afin d'envoyer et de recevoir des messages sécurisés de la part d'expéditeurs Vaultlet à l'avenir.

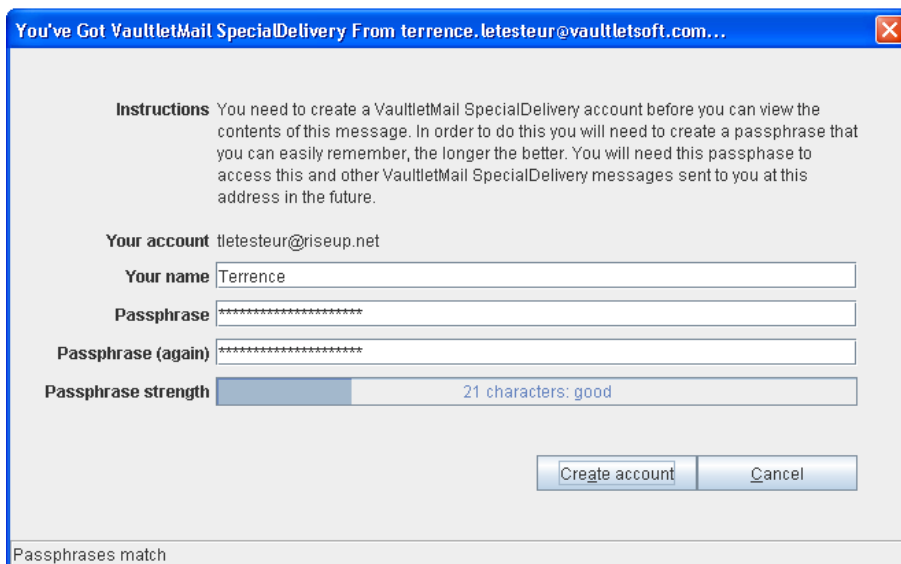


Figure 40 : La fenêtre You've Got VaultletMail SpecialDelivery From ...

**Quatrième étape. Saisissez** le nom d'utilisateur et la phrase secrète de votre nouveau compte.

**Commentaire :** Vous ne créez pas un compte de **courriel** sur le serveur de VS2Go. Vous ne faites qu'enregistrer votre adresse de courriel actuelle de telle sorte que vous pourrez dorénavant communiquer de façon sécurisée avec des correspondants qui disposent d'un compte VS2Go.

**Cinquième étape. Cliquez** sur :

**Sixième étape. Acceptez** le Contrat d'utilisation pour continuer.

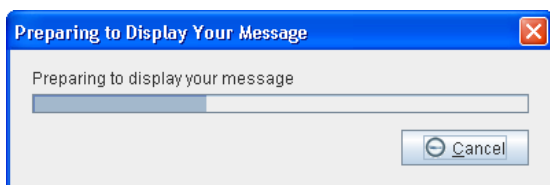


Figure 41 : La fenêtre Preparing to Display Your Message

La dernière étape consiste à confirmer le code secret créé par l'auteur du message pour le protéger.

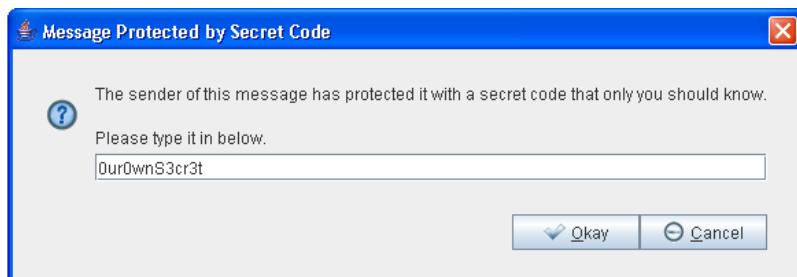


Figure 42 : La fenêtre Message Protected by Secret Code

**Septième étape. Saisissez** le code secret pour afficher le message original :

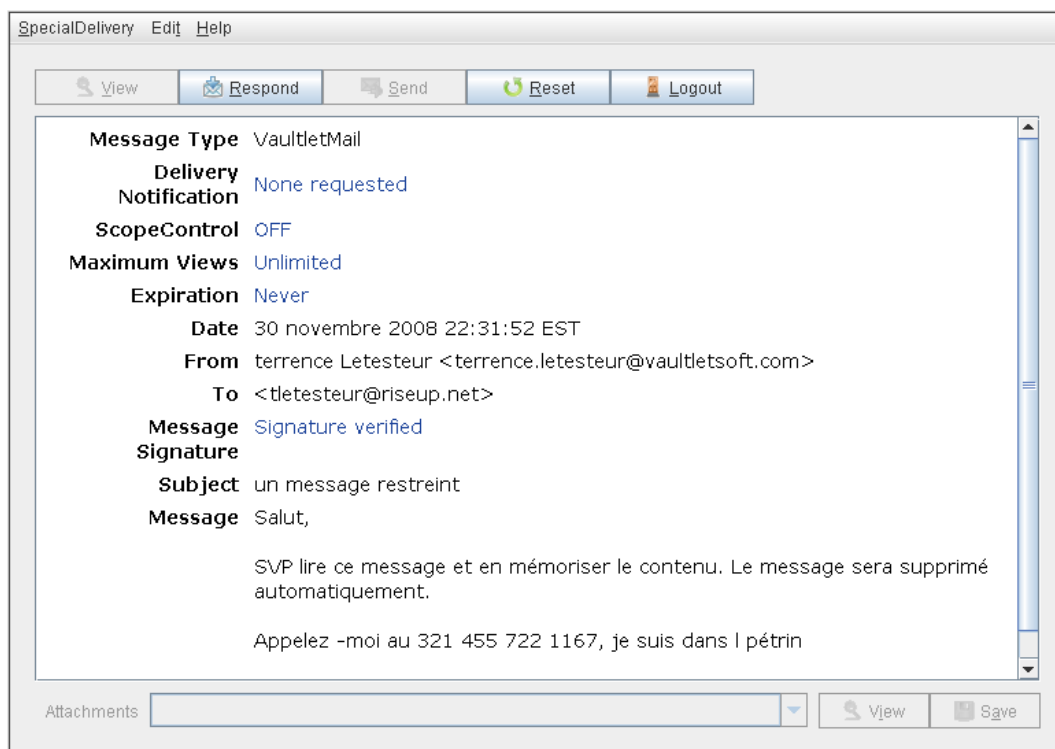


Figure 43 : L'affichage du message après avoir saisi le code secret

Vous pouvez désormais répondre au message de façon sécurisée en utilisant le bouton *Respond* sur cette même fenêtre. Toutes les communications subséquentes entre vous et ce correspondant seront beaucoup plus simples. Vous n'aurez qu'à ouvrir le lien inclus dans le message et à vous connecter avec les renseignements déjà créés. Vous n'aurez plus jamais à saisir de codes secrets suite à cette première opération.

## Faq et questions récapitulatives

VS2Go comporte plusieurs autres fonctions qui ne sont pas abordées dans ce guide. Vous pouvez toujours vous référer à la VaultMail Tips Page (Page de conseils) et aux FAQs pour plus de renseignements.

Même si cet outil ne semble pas particulièrement simple de prime abord, le programme VaultletSuite 2 Go a été conçu et développé avec minutie pour être facile d'utilisation. Les développeurs travaillent constamment à améliorer l'interface et la fonctionnalité du programme. C'est l'un des seuls services de courrier électronique gratuits offrant une fonction de chiffrement des messages et fichiers. La capacité d'envoyer des messages chiffrés à l'extérieur du domaine VaultletSoft peut s'avérer fort importante dans le cadre d'une stratégie de communication sécurisée.

Claudia et Pablo ont passé une bonne partie de la journée à utiliser VS2Go. Ils ont réussi à se créer chacun un compte et ont pu échanger des messages chiffrés. Cependant, Pablo a encore quelques questions :

**Q. :** *Si je crée un compte pour utilisateurs itinérants et que je choisis la méthode Simplicité pour stocker ma clé privée, de quoi ai-je besoin pour accéder à mon compte à partir de n'importe quel ordinateur?*

**R. :** *Tu auras besoin de la phrase secrète du compte pour te connecter et voir tes messages qui sont stockés sur le serveur de VaultletSoft. Si tu souhaites accéder à tes fichiers et archives, alors tu auras aussi besoin de ta clé USB.*

**Q. :** *Que se passe-t-il si j'oublie ou perds l'un ou l'autre de mes mots de passe pour accéder au compte?*

**R. :** *Cela pose un problème, parce que la méthode de chiffrement VS2Go repose sur l'utilisation de la phrase secrète. Si tu demandes à ce que ta phrase secrète soit réinitialisée, tu perdras automatiquement l'accès à tous les messages et fichiers chiffrés envoyés et reçus préalablement, et stockés dans le VaultletFiler. Tu recevras un code de connexion temporaire à ton adresse de rechange, ce qui te permettra tout de même de continuer à utiliser ton adresse de courriel VaultletSoft. VS2Go générera alors une nouvelle paire de clés, à partir de ta nouvelle phrase secrète, que le système utilisera dorénavant pour chiffrer ton compte.*

**Q. :** *Je veux m'assurer qu'une adresse de courriel de rechange soit associée à mon compte. Peux-tu me rappeler ce que je dois faire?*

**R. :** *Tu n'as qu'à te connecter à ton compte et sélectionner l'option Voir l'information du compte, à partir du menu Mon compte.*

**Q. :** *Je suis encore un peu incertain quant à certaines options du processus d'enregistrement.*

**R. :** *Si tu n'es pas certain, essaie la procédure d'enregistrement Simplicité - Rapide et facile. Le programme stockera tes archives sur ton ordinateur et ta clé privée sur un serveur de VaultletSoft. Tout ce que tu as à faire est de ne pas oublier ta phrase secrète, et te rappeler que tu ne peux accéder à ton compte qu'à partir de cet ordinateur.*

**Q. :** *Mon compte Bleu est enregistré pour un an seulement. Que se passera-t-il à la fin de cette période?*

**R. :** *Il existe plusieurs moyens de prolonger la durée de vie d'un compte Bleu. Tu peux payer, bien sûr. Tu peux aussi demander à trois personnes de créer des comptes VS2Go en utilisant ton adresse de courriel comme référent. Sinon, tu peux aussi saisir un Code Promo, que tu pourras trouver dans la copie physique de NGO in a Box - Security Edition. Si tu*

sélectionnes l'option Voir l'information du compte, à partir du menu Mon compte, tu peux choisir celle de ces méthodes qui te convient le mieux. Par ailleurs, tu peux sélectionner l'option Contactez-nous, à partir du menu Aide, et écrire directement à VaultletSoft pour demander une prolongation de la durée de vie de ton compte.

**Q.** : J'ai peur que mes correspondants soient réticents à passer par la procédure Special Delivery pour voir mes messages chiffrés.

**R.** : Tu as peut-être raison. Malheureusement la plupart des gens ont tendance à être moins préoccupés par les enjeux de sécurité qu'ils le devraient, et sont souvent réticents à acquérir de nouveaux outils. Certains de tes correspondants te demanderont peut-être de renvoyer tes messages en utilisant une méthode moins sûre. C'est à toi de déterminer si tu es prêt à mettre ta propre sécurité en danger. Sinon, tu devras convaincre tes correspondants que la confidentialité des communications est assez importante pour que l'on supporte des inconvénients mineurs. Évidemment, tu peux toujours les diriger vers le livret pratique de Security in-a-Box ou le manuel Digital Security and Privacy for Human Rights Defenders.

**Q.** : Disons que je reçois un message Special Delivery et que je suis capable de le déchiffrer à même mon navigateur Internet. Si je réponds à ce message, en cliquant sur le bouton Répond à partir de la même fenêtre, est-ce que la communication est toujours sécurisée?

**R.** : Oui. Le but de cette procédure (c.-à-d. télécharger et lancer cette application Java, créer un nom de compte et une phrase secrète, et ouvrir le message à partir d'un lien) est de conserver tous les éléments nécessaires à une communication chiffrée. Ta réponse, ainsi que tous les messages subséquents échangés par la fonction Special Delivery, seront sécurisés.

## 5.1 Questions récapitulatives

- En quoi VS2Go est-il plus sûr qu'un compte de courriel normal?
- Quels sont les trois éléments que vous devez avoir avec vous (et sur votre ordinateur) pour être en mesure d'accéder à votre compte VS2Go?
- Comment pouvez-vous modifier des fichiers stockés dans le FileVault?
- Comment pouvez-vous transférer des messages à partir des serveurs VaultletSoft vers votre ordinateur ou votre dispositif de stockage amovible?
- Quelle est la différence entre HalfLife et Scope Control?
- Si vous avez envoyé un message avec des restrictions concernant la durée de vie ou le nombre limite d'affichages, que s'affiche-t-il dans l'en-tête de l'Objet lorsque votre destinataire reçoit le message?

## Thunderbird - client de courriel sécurisé

### Short Description:

**Mozilla Thunderbird** est un client de messagerie électronique gratuit, de source ouverte, qui permet de recevoir, envoyer et archiver vos courriels. Vous pouvez gérer plusieurs comptes de courrier électronique à l'aide d'un programme unique. **Enigmail** et **GnuPG** vous offrent des options supplémentaires, dont l'authentification, la signature numérique et le chiffrement de vos messages, ce qui accroît la confidentialité et la sécurité de vos communications par courrier électronique.

### Online Installation Instructions:

#### Pour télécharger Thunderbird, Enigmail et GnuPG

- Lisez la courte introduction aux [Guides pratiques](#) <sup>[1]</sup>
- Cliquez sur l'icône **Thunderbird** ci-dessous pour ouvrir la page Internet [www.mozilla.com/thunderbird](http://www.mozilla.com/thunderbird)
- Cliquez sur le lien **Téléchargement gratuit** pour sauvegarder le fichier d'installation sur votre ordinateur; localisez ensuite le fichier, puis **double-cliquez** dessus
- Cliquez sur l'icône **Enigmail** ci-dessous pour ouvrir la page [www.enigmail.mozdev.org/download](http://www.enigmail.mozdev.org/download)
- Cliquez à droite sur le lien **Download v1.1.2 for Thunderbird 3.1** et sauvegardez le module complémentaire sur votre **Bureau**
- Cliquez sur l'icône **GnuPG** ci-dessous pour ouvrir la page [www.gnupg.org/download](http://www.gnupg.org/download)
- Faites dérouler la page jusqu'à la section **Binaries**, puis cliquez sur le lien **FTP** associé à l'option **GnuPG 1.4 compiled for Microsoft Windows**, puis sauvegardez le fichier d'installation sur votre ordinateur
- Poursuivez la lecture de la **Section 4.1** de ce guide pratique **Thunderbird pour installer Enigmail et GnuPG**
- Si vous avez sauvegardé les exécutables et les fichiers d'extension sur votre ordinateur, vous pouvez les supprimer après l'installation.

### Thunderbird: Enigmail: GnuPG:



[166]

ENIGMAIL

[167]



[168]

### Site Internet

- [www.mozilla.com/thunderbird](http://www.mozilla.com/thunderbird) <sup>[169]</sup>
- [www.enigmail.mozdev.org](http://www.enigmail.mozdev.org) <sup>[170]</sup>
- [www.gnupg.org](http://www.gnupg.org) <sup>[171]</sup>

### Configuration requise

- Compatible avec toutes les versions de Windows

### Versions utilisées pour rédiger ce guide

- Thunderbird 3.1.5
- Enigmail 1.1.2
- GNU Privacy Guard (GnuPG) 2.0.4



## Licence

- FLOSS (Free/Libre Open Source Software)

## Lecture préalable

- Livret pratique Security in-a-box, chapitre **7. Préserver la confidentialité de vos communications sur Internet** <sup>[126]</sup>

Niveau: 1: Débutant, 2: **Moyen** et 3: **Intermédiaire**, 4: Expérimenté, 5: Avancé

Temps d'apprentissage: 40 minutes

### Ce que vous apportera l'utilisation de cet outil:

- La capacité de gérer plusieurs comptes de courrier électronique à l'aide d'un seul et unique programme.
- La capacité de lire et composer des messages lorsque vous n'êtes pas connecté à Internet.
- La capacité d'utiliser le chiffrement par clé publique (asymétrique) pour faire en sorte que vos courriels restent confidentiels.

### Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

Le client de messagerie **Mozilla Thunderbird** est disponible pour **GNU Linux, Mac OS, Microsoft Windows** et d'autres systèmes d'exploitation. En ce qui a trait à la sécurité numérique, la gestion simultanée de plusieurs comptes de courrier électronique est une tâche complexe, c'est pourquoi il est *fortement recommandé* d'utiliser **Mozilla Thunderbird** à cette fin. Les avantages que présente **Thunderbird**, un client de messagerie *libre et gratuit*, multi plateforme et de *source ouverte*, sont d'autant plus importants lorsqu'on le compare à ses rivaux commerciaux comme **Microsoft Outlook**. Cela dit, si vous préférez utiliser un autre programme que **Mozilla Thunderbird**, nous recommandons les trois options suivantes, également gratuites et de source ouverte:

- **Claws Mail** <sup>[172]</sup> disponible pour **GNU Linux** et **Microsoft Windows**;
- **Sylpheed** <sup>[173]</sup> disponible pour **GNU Linux, Mac OS** et **Microsoft Windows**;
- **Alpine** <sup>[174]</sup> disponible pour **GNU Linux, Mac OS** et **Microsoft Windows**.

## 1.1 À propos de cet outil

**Mozilla Thunderbird** est un client de messagerie électronique libre, gratuit, multi plateforme et de source ouverte, qui permet de recevoir, envoyer, trier et archiver des messages de courrier électronique. Un client de messagerie est une application informatique qui vous permet de télécharger et gérer vos courriels sans utiliser un navigateur Internet. Vous pouvez gérer plusieurs comptes de courriel à l'aide d'un seul et unique programme de messagerie. Vous devez avoir au moins un compte de courrier électronique pour utiliser **Thunderbird**. Vous pouvez également créer des comptes **Gmail** <sup>[175]</sup> ou **RiseUp** <sup>[176]</sup> si vous le souhaitez.

**Enigmail** est un module complémentaire conçu pour **Thunderbird**. Il donne accès aux fonctions d'authentification et de chiffrement offertes par **GNU Privacy Guard (GnuPG)**.

**GnuPG** est un programme de chiffrement par clé publique (asymétrique) utilisé pour générer et gérer des paires de clés afin de chiffrer et déchiffrer des messages pour préserver la confidentialité et la sécurité de vos communications par courrier électronique. Comme nous le verrons plus loin dans ce chapitre, **GnuPG** doit être installé pour qu'**Enigmail** fonctionne.

### Offline Installation Instructions :

#### Pour installer Thunderbird, Enigmail, GPG

- \*Lisez la courte **Introduction** aux **Guides pratiques** <sup>[1]\*\*</sup>
- **Cliquez sur l'icône Thunderbird, Enigmail, GPG ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.

Thunderbird: Enigmail: GnuPG:



<sup>[177]</sup>

ENIGMAIL

<sup>[178]</sup>



<sup>[179]</sup>

# Comment installer Thunderbird


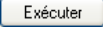
Sommaire des sections de cette page:

- **2.0 Comment installer Thunderbird**
- **2.1 Comment désactiver l'option Recherche et indexation globales dans Thunderbird**
- **2.2 Comment enregistrer un compte de courrier électronique dans Thunderbird**
- **2.3 Comment enregistrer des comptes de Blogs, de nouvelles et de Groupes de discussion dans Thunderbird**

---

## 2.0 Comment installer Thunderbird

L'installation de **Thunderbird** est un processus relativement simple et rapide. Pour lancer l'installation de **Thunderbird**, suivez les étapes énumérées ci-dessous:

**Première étape.** Double-cliquez sur  Thunderbird Setup 3.1.7 ; il est possible que la boîte de dialogue de confirmation *Fichier ouvert - Avertissement de sécurité* s'affiche à ce moment. Si c'est le cas, cliquez sur  pour afficher la fenêtre suivante:

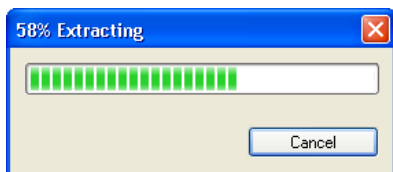


Figure 1: La barre de progression de l'extraction

Lorsque l'extraction des fichiers de **Thunderbird** est complétée, la fenêtre *Bienvenue dans l'assistant d'installation de Mozilla Thunderbird* apparaît.

**Deuxième étape.** Cliquez sur  pour activer la fenêtre *Mozilla Thunderbird - Type d'installation*.

**Troisième étape.** Cliquez sur  pour accepter les réglages par défaut et afficher la fenêtre suivante:

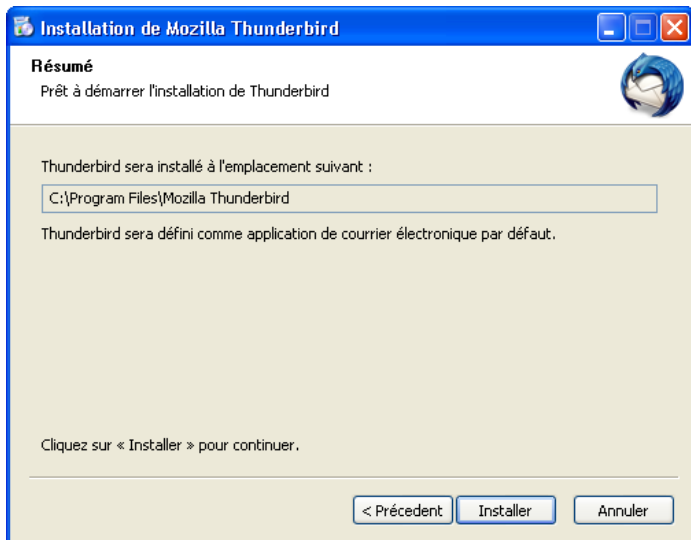



Figure 2: La fenêtre Mozilla Thunderbird - Résumé

**Quatrième étape.** Cliquez sur  pour lancer le processus d'installation. La barre de progression **Mozilla Thunderbird - Installation** s'affiche alors. Lorsque le processus d'installation est terminé, la fenêtre suivante s'affiche:

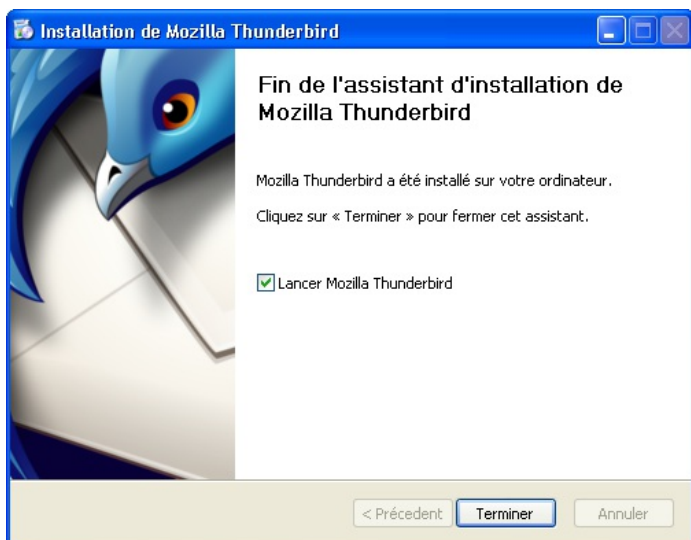


Figure 3: La fenêtre Fin de l'assistant d'installation de Mozilla Thunderbird

**Cinquième étape.** Cliquez sur  pour compléter le processus d'installation.

**Astuce:** **Thunderbird** se lancera automatiquement si l'option *Lancer Mozilla Thunderbird* est cochée, tel qu'illustré à la figure 3 ci-dessus. Pour lancer le programme à l'avenir, vous pouvez, soit **double-cliquer** sur l'icône de bureau de **Thunderbird**, soit sélectionner > Programmes > Mozilla Thunderbird > Mozilla Thunderbird.

## 2.1 Comment désactiver l'option Recherche et indexation globales dans Thunderbird

**Attention:** La fonction *Recherche et indexation globales* de **Thunderbird** doit être désactivée pour optimiser la performance du programme. Selon la quantité et la taille de vos messages, cette fonction peut ralentir votre système et réécrivait continuellement et inutilement les mêmes données sur votre disque dur. Au fur et à mesure que votre disque dur se remplit, plusieurs opérations de votre système tourneront de plus en plus au ralenti.

Pour désactiver l'option *Recherche et indexation globales*, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez **Outils > Options** dans la console **Thunderbird** pour afficher la fenêtre *Options*.



**Deuxième étape.** Cliquez sur **Avancé** pour afficher le contenu de cet onglet:

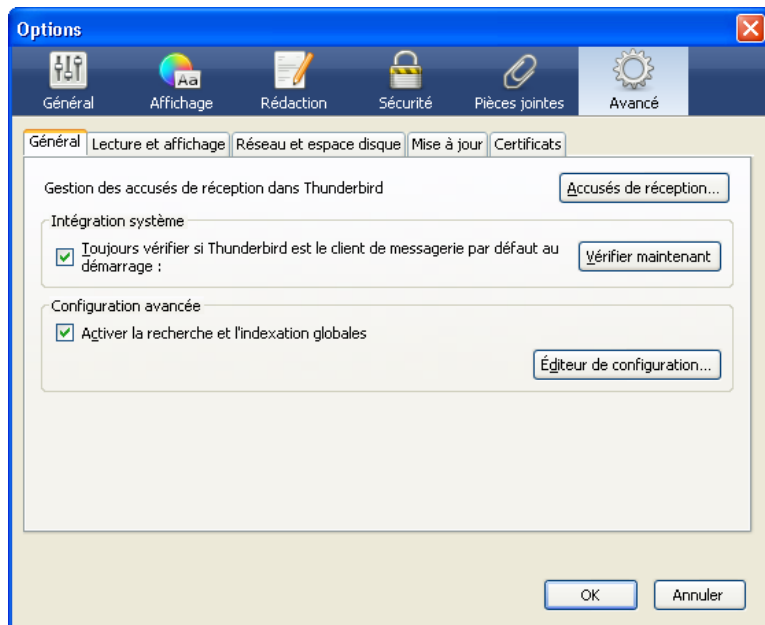


Figure 4: La fenêtre *Options* affichant le contenu de l'onglet *Avancé*

**Troisième étape.** Cliquez sur la case *Activer la recherche et l'indexation globales*, dans la section *Configuration avancée*, pour désactiver cette option, tel qu'illustré ci-dessous:

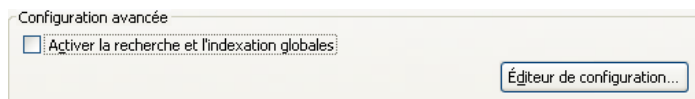


Figure 5: La section *Configuration avancée*

Maintenant que vous avez désactivé cette option, vous êtes prêt à enregistrer un compte de courrier électronique dans **Thunderbird**.

## 2.2 Comment enregistrer un compte de courrier électronique dans Thunderbird

La fenêtre *Assistant d'importation - Importer les paramètres et les dossiers de messages* n'apparaît qu'à la première installation de **Thunderbird**.

**Première étape.** Cochez l'option *Ne rien importer*, tel qu'illustré ci-dessous:

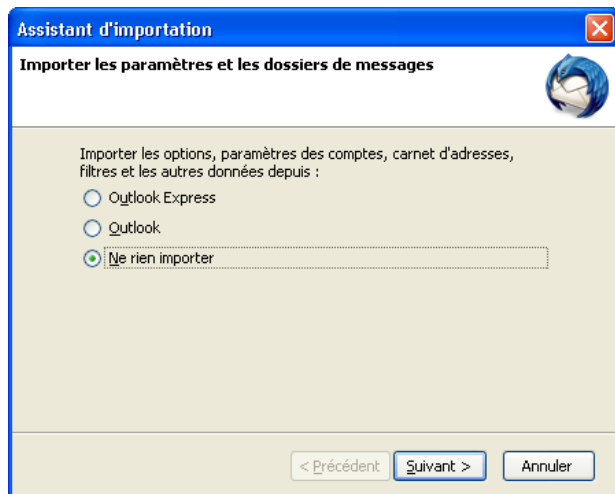


Figure 6: L'*Assistant d'importation - Importer les paramètres et les dossiers de messages*

Deuxième étape. Cliquez sur  pour afficher la fenêtre suivante:

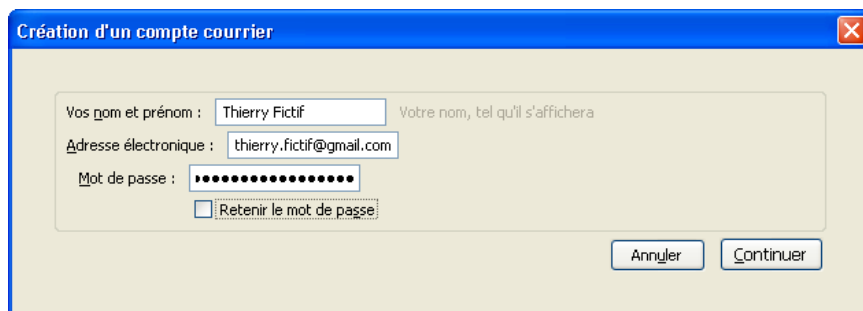


Figure 7: La fenêtre *Création d'un compte courrier*

Troisième étape. Saisissez votre nom, adresse de courrier électronique et mot de passe dans les champs appropriés; puis **décochez** l'option *Retenir le mot de passe*, tel qu'illustré à la figure 7 ci-dessous.

Quatrième étape. Cliquez sur  pour afficher la fenêtre suivante:

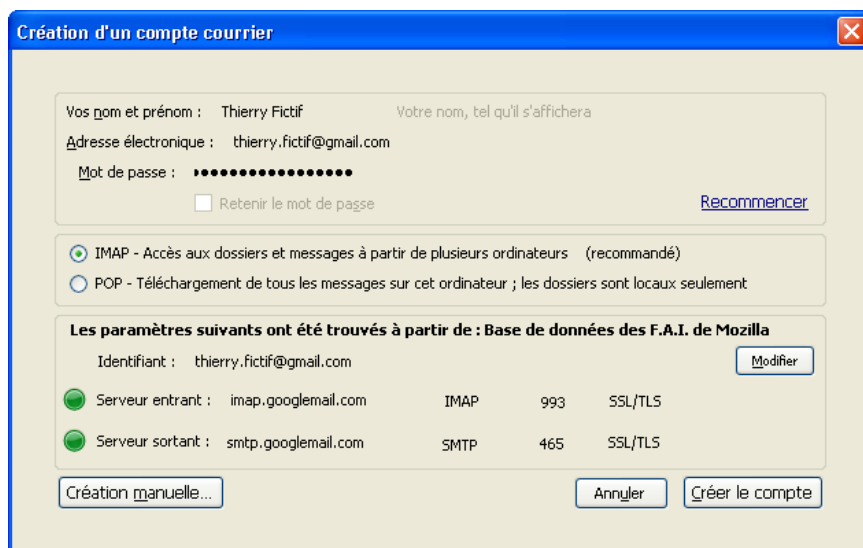


Figure 8: La fenêtre *Création d'un compte courrier* avec l'option **IMAP - Accès aux dossiers et messages à partir de plusieurs ordinateurs** sélectionnée

## IMAP et POP: Descriptions et utilisation

**Internet Message Access Protocol (IMAP)** et **Post Office Protocol (POP)** sont deux méthodes distinctes d'archiver et de recevoir des messages de courrier électronique.

- **Internet Message Access Protocol (IMAP):** Lorsque vous utilisez la méthode **IMAP**, tous vos dossiers (y compris les dossiers *Courrier entrant*, *Brouillons*, *Envoyés*, *Corbeille* et tous les autres dossiers) demeure sur le serveur de courrier. De cette façon, vous pouvez accéder à ces dossiers depuis un autre ordinateur. Tous les messages seront donc conservés sur le serveur et, initialement, seulement le titre des messages (comportant des renseignements comme la date et l'heure, le sujet du message, le nom de l'expéditeur, etc.) sont téléchargés pour être affichés par votre client mail sur votre ordinateur. Les messages complets ne sont affichés que lorsque vous cliquez dessus pour les ouvrir. **Thunderbird** peut aussi être configuré pour archiver dans votre ordinateur des copies de vos messages qui se trouvent dans certains ou dans tous vos dossiers, afin que vous puissiez travailler dessus en mode autonome (non connecté à Internet). En mode **IMAP**, lorsque vous supprimez des messages ou des dossiers, vous le faites *à la fois* sur votre ordinateur local et sur le serveur.
- **Post Office Protocol (POP):** Lorsque vous utilisez la méthode **POP**, seul le dossier *Courrier entrant* (le dossier où sont livrés et affichés les nouveaux messages entrants) demeure sur le serveur distant; tous les autres dossiers sont situés sur votre ordinateur local seulement. Vous pouvez choisir de laisser vos messages dans le dossier *Courrier entrant* sur le serveur après les avoir téléchargés sur votre ordinateur, ou vous pouvez les supprimer du serveur. Dans le dernier cas, si vous accédez à votre compte depuis un autre ordinateur, vous ne verrez uniquement que les messages du dossier *Courrier entrant* (les nouveaux messages et ceux que vous avez choisi de ne pas supprimer du serveur).

Cinquième étape. Cliquez sur  pour créer votre compte et afficher la console **Thunderbird** avec votre compte de courrier compris dans la barre *Tous les dossiers*, à gauche, tel qu'illustré ci-dessous:

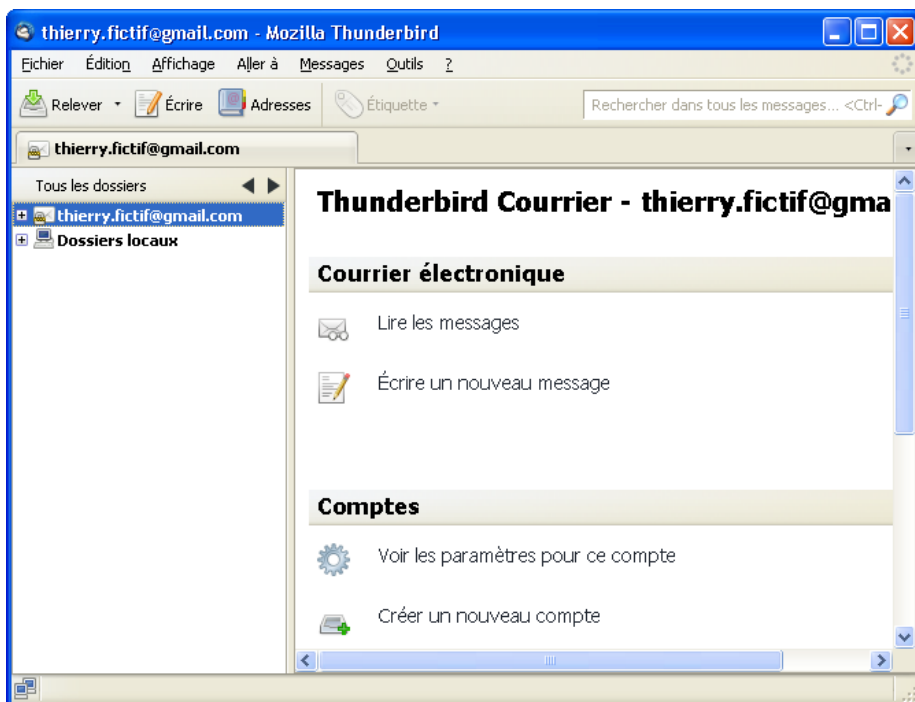


Figure 9: L'interface principale de Thunderbird affichant votre compte Gmail nouvellement enregistré

**Commentaire:** Pour ajouter un autre compte de courriel, **sélectionnez Fichier > Nouveau > Comptes courrier...** pour afficher la *figure 7* de cette section, et reprenez les **étapes 3 à 5**.

Après avoir enregistré vos comptes de courrier électronique dans **Thunderbird**, la prochaine fois que vous ouvrirez l'interface principale, on vous demandera de saisir votre mot de passe pour chaque compte, comme suit:

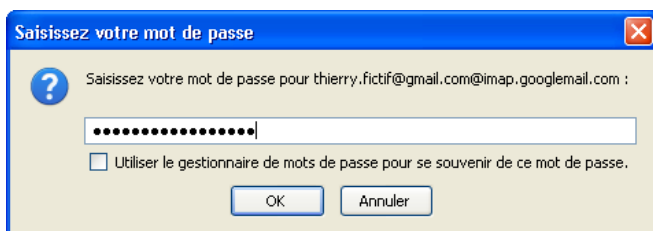



Figure 10: La fenêtre Saisissez votre mot de passe

**Commentaire:** Bien que la fonction d'enregistrement du mot de passe ne soit généralement pas recommandée, **Thunderbird** comporte une fonction de *Mot de passe maître*. Cette fonction permet de n'utiliser qu'un seul mot de passe pour protéger tous les mots de passes associés à vos différents comptes, que vous ne saisissez qu'une seule fois lors du processus d'enregistrement. Pour plus de renseignements sur cette fonction, veuillez consulter la section **3.3 Comment configurer les onglets de sécurité dans Thunderbird** <sup>[180]</sup> - L'onglet **Mot de passe**.

## 2.3 Comment enregistrer des comptes de blogs, de nouvelles et de groupes de discussion

Pour créer et enregistrer un compte pour des blogs, des nouvelles ou des groupes de discussion, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez > **Fichier > Nouveau > Autres comptes** pour afficher la fenêtre *Assistant de création de compte > Paramétrage du nouveau compte*.

**Deuxième étape.** Cochez soit l'option *Blogs et nouvelles*, soit l'option *Groupes de discussion*, puis cliquez sur  pour afficher la fenêtre suivante:

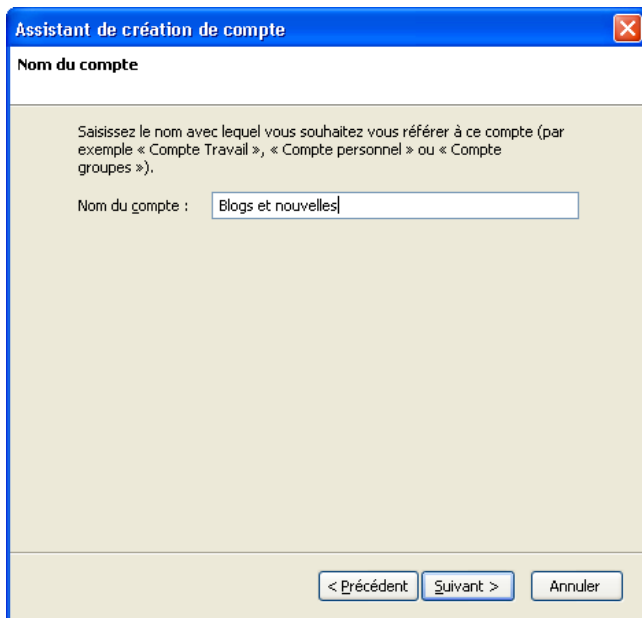


Figure 11: La fenêtre Assistant de création de compte - Nom du compte

Troisième étape. Cliquez sur  pour afficher la fenêtre suivante:

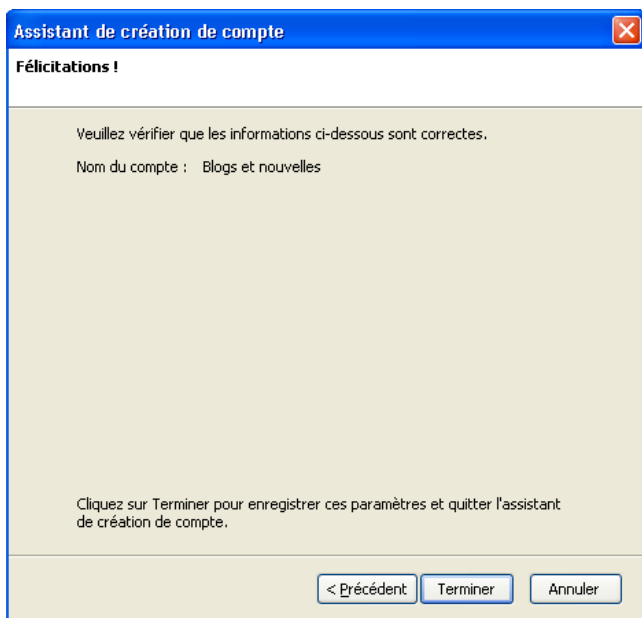


Figure 12: La fenêtre Assistant de création de compte - Félicitations!

Cinquième étape. Cliquez sur  pour compléter le processus d'enregistrement du compte et retourner à la console Thunderbird.

Maintenant que vous avez configuré **Thunderbird** pour une utilisation optimale, veuillez lire la prochaine section, **Comment régler les options de sécurité dans Thunderbird** <sup>[181]</sup>.

## Comment régler les options de sécurité dans Thunderbird

Sommaire des sections de cette page:

- **3.0 À propos des options de sécurité de Thunderbird**
- **3.1 Comment désactiver le panneau d'affichage des messages de Thunderbird**
- **3.2 Comment désactiver la fonction HTML dans Thunderbird**
- **3.3 Comment régler les options de sécurité dans Thunderbird**
- **3.4 Comment activer le filtre des indésirables dans les paramètres du compte**

---

### 3.0 À propos des options de sécurité de Thunderbird

Dans le contexte de **Mozilla Thunderbird**, le terme 'sécurité' fait référence à la protection de votre ordinateur contre des messages de courrier électronique nuisibles ou malveillants. Il peut s'agir de pourriel, par exemple, ou encore de messages servant de véhicules à des virus ou des logiciels espions. Il existe plusieurs paramètres qui doivent être activés,

désactivés ou réglés adéquatement dans **Mozilla Thunderbird** pour permettre au programme de défendre efficacement votre système contre des attaques provenant du courrier électronique. Il est également *absolument impératif* que vous installiez des logiciels pare-feu, antivirus et anti-mouchards.

Pour plus de renseignements sur les moyens de prévenir les intrusions nuisibles ou malveillantes, veuillez consulter le chapitre **1. Protéger votre ordinateur contre les logiciels malveillants et les pirates** [4] du **Livret pratique**, ainsi que les chapitres portant sur **Avast** [182], **Comodo Firewall** [183] et **Spybot** [184].

### 3.1 Comment désactiver le panneau d'affichage des messages de Thunderbird

La console **Thunderbird** est séparée en trois sections distinctes: l'encadré à gauche affiche les différents dossiers de vos comptes de courriel; le panneau à droite affiche une liste de messages; et le panneau du bas à droite affiche un *aperçu* d'un message sélectionné.

**Commentaire:** Si un message contient du code malicieux, ce panneau affichant l'aperçu du message pourrait l'activer; il est donc recommandé de le désactiver.

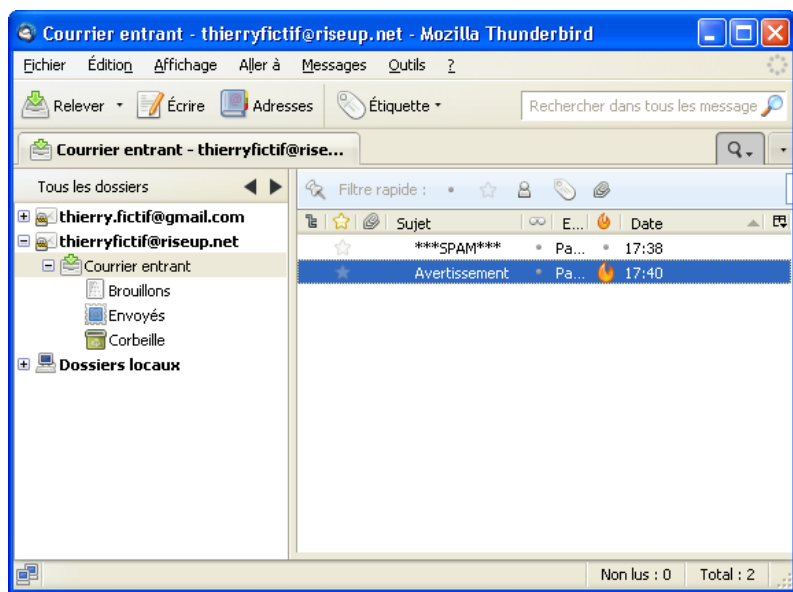


Figure 1: L'interface principale de Thunderbird

Pour désactiver le panneau d'affichage des messages, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez **Affichage > Disposition**, puis **désélectionnez** l'option *Panneau d'affichage des messages* pour la désactiver, comme suit:

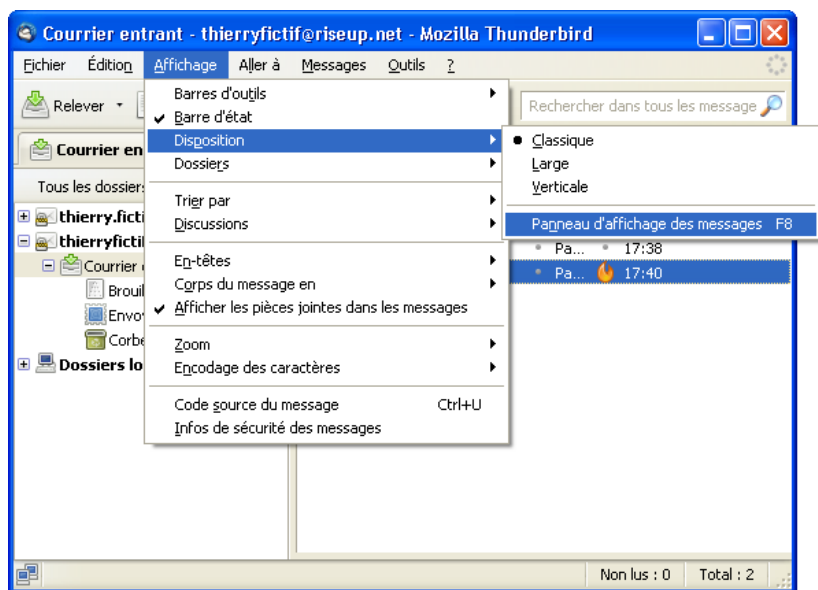


Figure 2: Le menu *Affichage* affichant le sous-menu *Disposition* avec le *Panneau d'affichage des messages* sélectionné

Le *Panneau d'affichage des messages* n'apparaîtra plus et vous devrez désormais **double-cliquer** sur un message pour en afficher le contenu. Si un message vous semble suspect (parce que son titre, par exemple, est impertinent ou inattendu, ou parce qu'il provient d'un expéditeur inconnu), vous pouvez maintenant le supprimer avant d'en afficher le contenu.

### 3.2 Comment désactiver la fonction HTML dans Thunderbird

**Thunderbird** vous permet d'utiliser le **HyperText Markup Language (HTML)** pour composer vos messages. Cela signifie

que vous pouvez recevoir ou envoyer des messages qui comprennent des couleurs, des polices spéciales, des images et d'autres options de mise en page. Par contre, le **HTML** est le même langage utilisé pour coder des pages Web; l'affichage de messages codés en **HTML** peut vous exposer à des codes malveillants, ce qui comporte certains des mêmes risques que ceux posés par les sites Internet.

Pour désactiver la fonction de mise en page **HTML**, suivez les étapes énumérées ci-dessous:

**Première étape. Sélectionnez Affichage > Corps du message en > Texte seul**, comme suit:

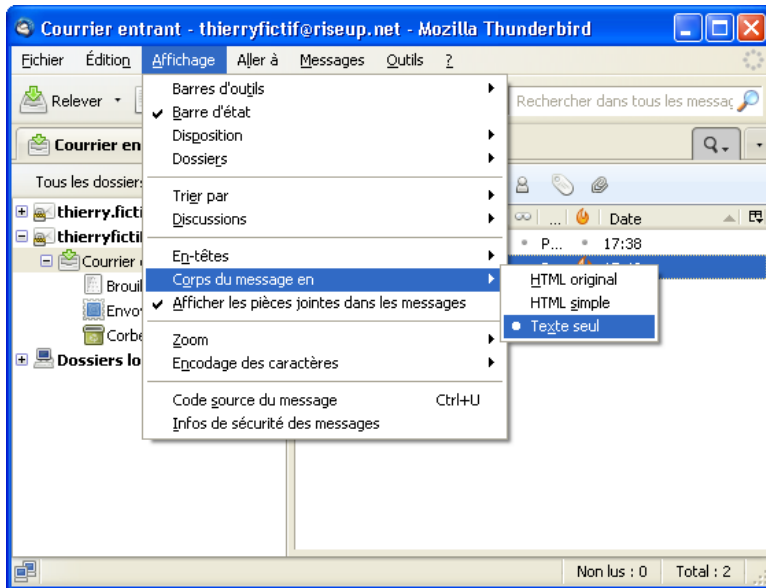


Figure 3: Le menu Affichage affichant le sous-menu Corps du message en avec l'option Texte seul sélectionné

### 3.3 Comment régler les options de sécurité

**Thunderbird** comporte deux filtres de courrier indésirable qui peuvent vous aider à déterminer quels messages sont des pourriels. Par défaut, ces filtres sont désactivés et vous devez donc les activer avant de les utiliser. Même après les avoir désactivés, vous continuerez à recevoir du courrier indésirable, mais **Thunderbird** les classera automatiquement dans le dossier *Indésirables*.


Le courrier frauduleux, aussi appelés messages *d'hammeçonnage*, ou *phishing*, essaie habituellement de vous faire cliquer sur des liens qui sont codés dans le message. Souvent, ces liens redirigent votre navigateur vers des sites Internet qui tenteront d'infecter votre ordinateur avec un virus. Dans d'autres cas, le lien vous mènera vers un site Internet qui semble légitime, mais qui est en fait conçu pour vous induire à révéler vos noms d'utilisateurs et vos mots de passe, qui pourront ensuite être utilisés ou vendus à une tierce partie à des fins commerciales ou malveillantes.

**Thunderbird** peut identifier ce type de courrier et vous en avertir. Des outils supplémentaires peuvent prévenir les infections provenant de sites Internet malveillants: voir la section **Autres modules utiles de Mozilla** <sup>[185]</sup> du chapitre portant sur **Firefox**.

Le premier ensemble de paramètres de sécurité concernant le courrier indésirable se trouve dans la fenêtre *Options - Sécurité*, où la majorité des options de sécurité et de confidentialité peuvent être réglées. Pour y accéder, suivez les étapes énumérées ci-dessous:

**Première étape. Sélectionnez Outils > Options** pour afficher la fenêtre *Options*.



**Deuxième étape. Cliquez sur**  **pour afficher la fenêtre suivante:**



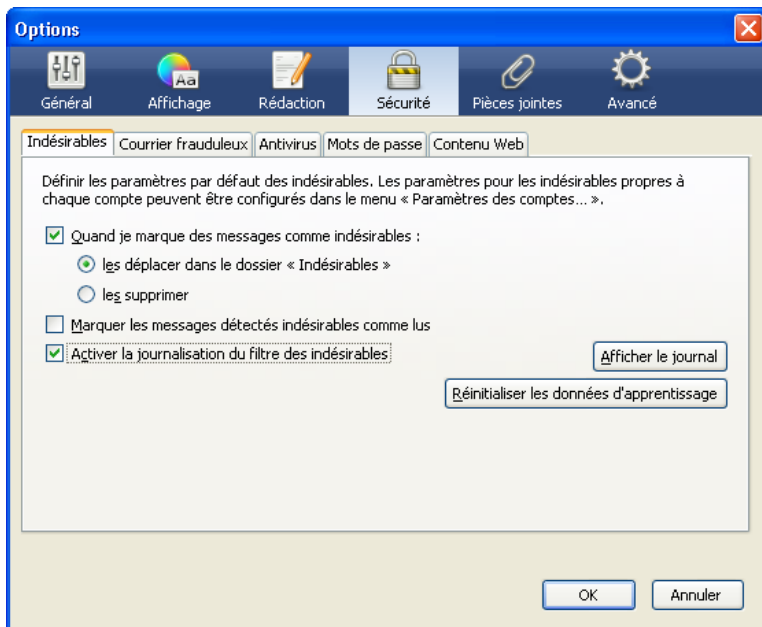


Figure 4: La fenêtre Sécurité affichant le contenu de l'onglet Indésirables

## L'onglet Indésirables

**Première étape.** Cochez les options pertinentes dans l'onglet *Indésirables*, tel qu'illustré à la *figure 4*, ci-dessus, pour permettre à **Thunderbird** de supprimer les messages que vous définis comme courrier indésirable. D'autres options de filtrage du courrier indésirable seront abordés plus loin dans cette section.

## L'onglet Courrier frauduleux

**Première étape.** Cochez l'option *Signaler si le message en cours de lecture est susceptible d'être frauduleux* pour permettre à **Thunderbird** d'analyser les messages pour y détecter des fraudes potentielles:

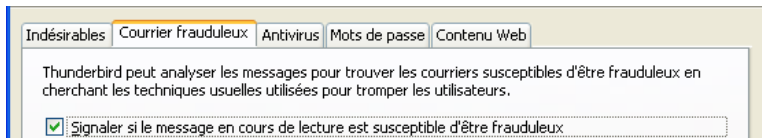


Figure 5: L'onglet Courrier frauduleux

## L'onglet Antivirus

**Première étape.** Cliquez sur l'onglet *Antivirus* pour afficher la fenêtre suivante:

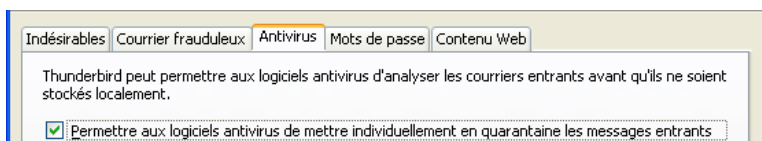


Figure 6: L'onglet Antivirus

Cette option permet à votre logiciel antivirus de scanner et d'isoler des messages individuellement au fur et à mesure qu'ils arrivent. Si cette option n'est pas activée, il est possible que votre dossier *Courrier entrant au complet* soit placé 'en quarantaine' si vous recevez ne serait-ce qu'un seul message infecté.

**Commentaire:** Il est tenu pour acquis qu'il y a un programme antivirus fonctionnel installé sur votre ordinateur. Veuillez consulter le chapitre portant sur **Avast** <sup>(26)</sup> pour plus de renseignements sur l'installation et la configuration d'un logiciel antivirus.

## L'onglet Mots de passe

**Première étape.** Cliquez sur l'onglet *Mots de passe* pour afficher la fenêtre suivante:

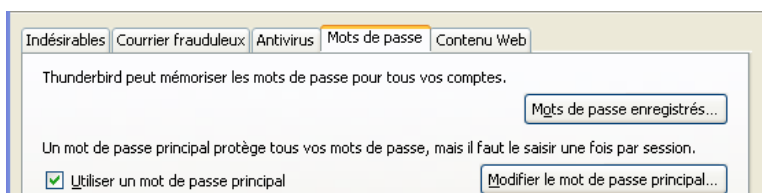


Figure 7: L'onglet Mots de passe

**Important:** Nous recommandons fortement que vous gardiez vos mots de passe privés en utilisant un programme conçu

spécialement à cette fin; veuillez consulter le chapitre portant sur **KeyPass** [82] pour plus de renseignements à ce sujet.

**Commentaire:** Les options de l'onglet *Mots de passe* ne fonctionneront que si vous sélectionnez d'abord l'option *Retenir le mot de passe* dans la toute première fenêtre d'enregistrement d'un compte courrier dans **Thunderbird**.

**Deuxième étape.** Cliquez sur  pour afficher la fenêtre suivante:



Figure 8: La fenêtre *Enregistrement des mots de passe*

La fenêtre *Enregistrement des mots de passe* vous permet de supprimer ou d'afficher les mots de passe correspondant à chacun de vos comptes. Cela dit, pour maximiser votre sécurité et la confidentialité de vos renseignements, vous pouvez également définir un *Mot de passe principal* pour faire en sorte que vos mots de passe ne soit pas accessibles aux personnes qui sont le moins familières avec les options de mots de passe de **Thunderbird**.

**Troisième étape.** Cochez l'option *Utiliser un mot de passe principal*, tel qu'illustré à la figure 7 pour activer le bouton *Modifier le mot de passe principal*.

**Quatrième étape.** Cliquez sur  pour afficher la fenêtre suivante:

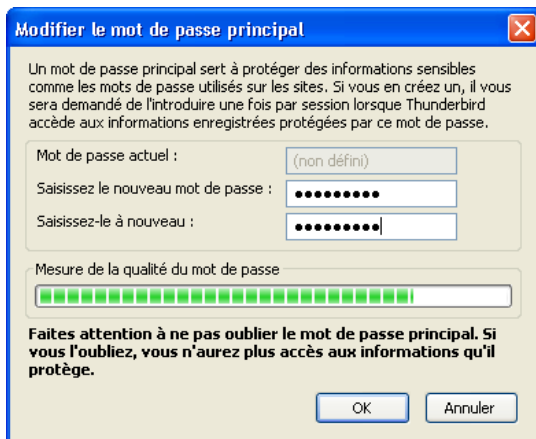


Figure 9: La fenêtre *Modifier le mot de passe principal*

**Cinquième étape.** Saisissez un mot de passe suffisamment difficile, que vous seul connaîtrez, puis cliquez sur  pour confirmer votre *Mot de passe principal*. La prochaine fois que vous cliquez sur , la fenêtre suivante apparaîtra pour vous demander de saisir votre mot de passe principal:

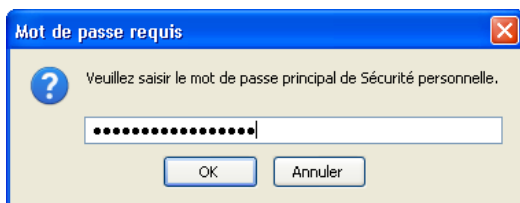


Figure 10: La fenêtre *Mot de passe requis*

## L'onglet *Contenu Web*

Un cookie est un minuscule texte codé que votre navigateur web utilise pour authentifier ou identifier un site Internet donné. L'onglet *Contenu Web* vous permet de spécifier quels cookies de blogs, de nouvelles ou de groupes de discussions sont sûrs et fiables.

**Première étape.** Cliquez sur l'onglet *Contenu Web* pour afficher la fenêtre suivante:

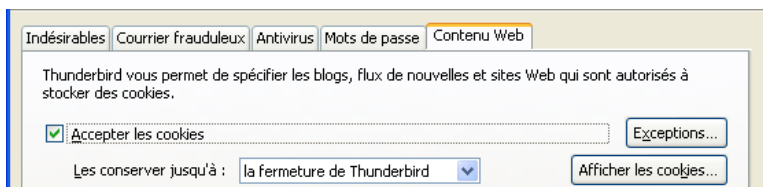


Figure 11: L'onglet Contenu Web

**Deuxième étape.** Sélectionnez l'option *la fermeture de Thunderbird* dans la liste *Les conserver jusqu'à:* pour supprimer les cookies lorsque vous fermez **Thunderbird**, pour une plus grande sécurité.

### 3.4 Comment activer le filtre des indésirables dans les paramètres du compte

Le deuxième type de filtrage du courrier indésirable offert par **Thunderbird** se trouve dans la fenêtre *Paramètres des comptes - Paramètres pour les indésirables*. Par défaut, ces filtres sont désactivés et vous devrez donc les activer pour les utiliser. Lorsque des messages indésirables arrivent, **Thunderbird** les classera automatiquement dans les dossiers *Indésirables* associés à chaque compte.

**Première étape.** Sélectionnez **Outils > Paramètres des comptes** pour afficher la fenêtre *Paramètres des comptes*.

**Deuxième étape.** Sélectionnez l'option *Paramètres des indésirables* associé à un compte **Gmail** ou **RiseUp** dans l'encadré de gauche.

**Troisième étape.** Réglez les options des *Paramètres des indésirables* de sorte que vos *Paramètres de comptes - Paramètres des indésirables* ressemblent à ceci:

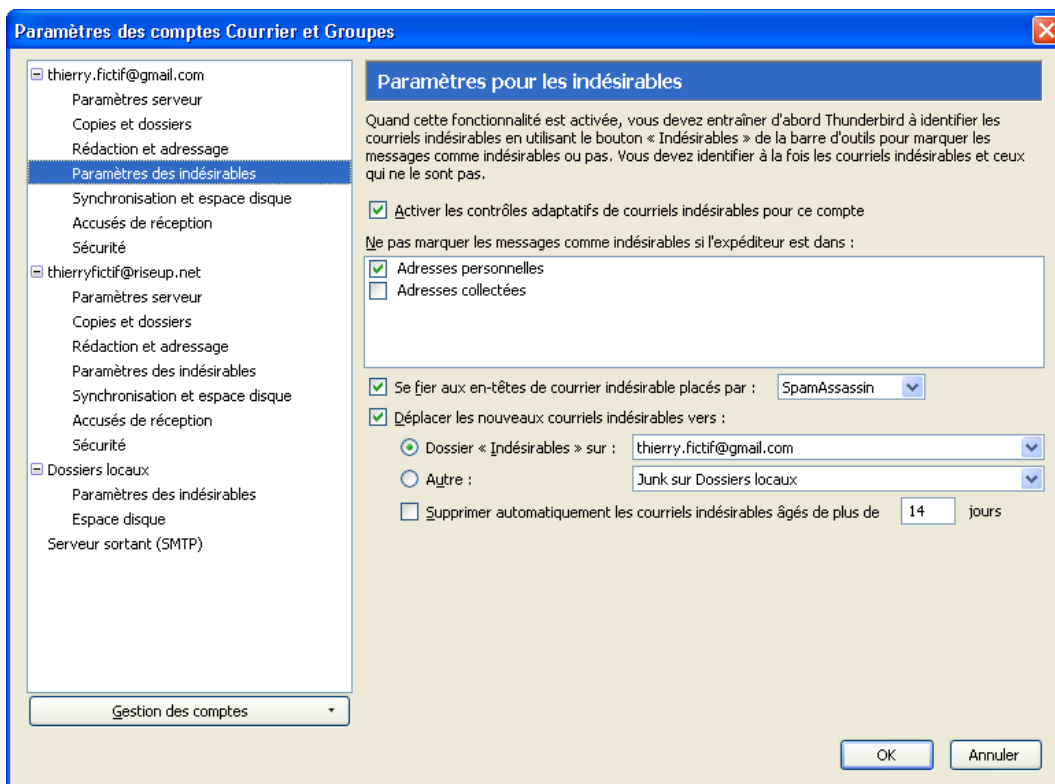


Figure 12: La fenêtre Paramètres des comptes - Paramètres des indésirables

**Quatrième étape.** Cliquez sur  pour compléter la configuration de la fenêtre *Paramètres des comptes*.

**Commentaire:** Les options des *Paramètres des indésirables* doivent être réglés séparément pour chaque compte. Ainsi, les indésirables des compte *Gmail* ou *Riseup* seront placés dans leur dossier *Supprimés* respectif. Sinon, vous pouvez également désigner un *Dossier local* pour recevoir les indésirables de tous vos comptes.

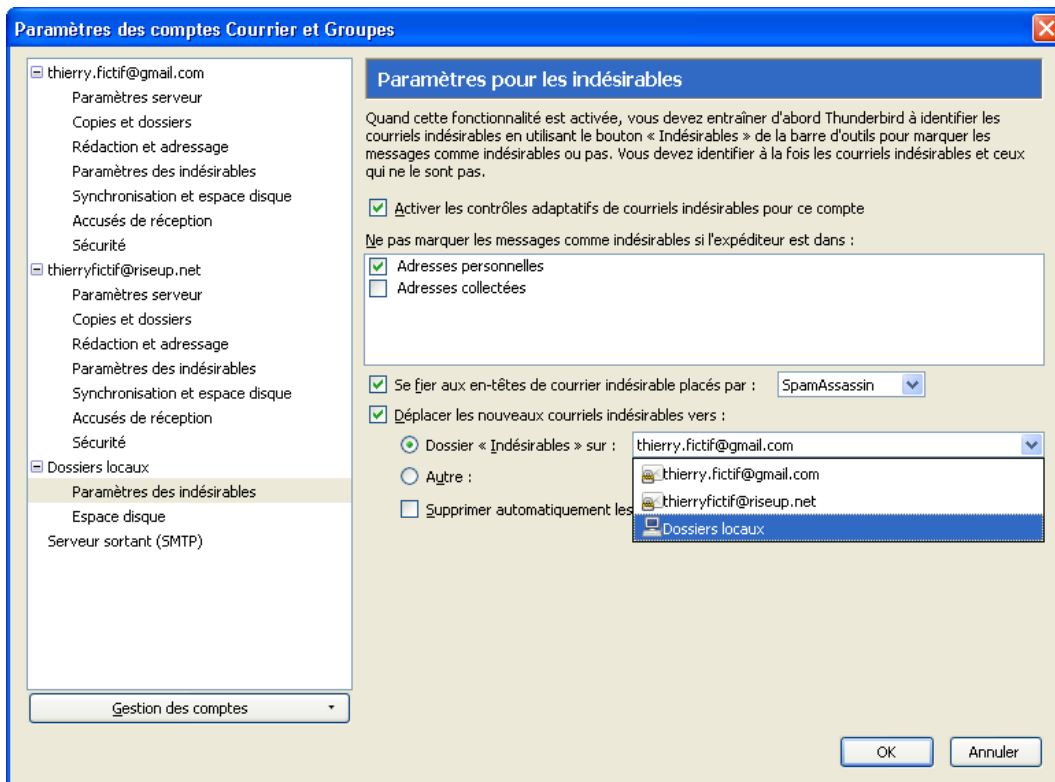


Figure 13: La fenêtre Paramètres des comptes - Paramètres des indésirables affichant les réglages pour un dossier Indésirables central

**Première étape.** Sélectionnez l'option *Paramètres des indésirables* sous la rubrique *Dossiers locaux* dans l'encadré de gauche.

**Deuxième étape.** Sélectionnez l'option *Dossiers locaux* dans la liste défilante *Dossier Indésirables sur:*, tel qu'illustré à la figure 13.

**Troisième étape.** Cliquez sur  pour compléter la configuration de la fenêtre *Paramètres des comptes*.

Maintenant que vous avez configuré les diverses options de sécurité et de gestion des indésirables de **Thunderbird**, veuillez lire la prochaine section, [Comment utiliser Enigmail avec GnuPG dans Thunderbird](#) <sup>[186]</sup>.

## Comment utiliser Enigmail avec GnuPG dans Thunderbird

Sommaire de sections de cette page:

- [4.0 Un aperçu d'Enigmail, de GnuPG et du chiffrement asymétrique \(à clé privée\)](#)
- [4.1 Comment installer Enigmail et GnuPG](#)
- [4.2 Comment générer des paires de clés et configurer Enigmail pour qu'il fonctionne avec vos comptes de courriel](#)
- [4.3 Comment échanger des clés publiques](#)
- [4.4 Comment valider et signer un paire de clés](#)
- [4.5 Comment chiffrer et déchiffrer des messages](#)

---

### 4.0 Un aperçu d'Enigmail, de GnuPG et du chiffrement asymétrique (à clé privée)

**Enigmail** est un module complémentaire de **Mozilla Thunderbird** qui vous permet de protéger la confidentialité de vos communications par courrier électronique. **Enigmail** n'est rien d'autre qu'une interface graphique conçue pour faciliter l'utilisation du programme de chiffrement **GnuPG** avec **Thunderbird**. L'interface d'**Enigmail** est représentée par un lien *OpenPGP* dans la barre d'outils de la console **Thunderbird**.

**Enigmail** emploie la méthode de **cryptographie asymétrique, ou cryptographie à clé publique** <sup>[187]</sup>. En vertu de cette méthode, chaque individu doit générer sa propre paire de clés. La première clé est dite *privée*. Celle-ci est protégée par un mot de passe complexe, gardée secrète et *jamais* partagée avec *qui que ce soit*.

La deuxième clé est dite *publique*. Cette clé peut être partagée avec vos correspondants. Lorsque vous avez la *clé publique* d'un correspondant, vous pouvez commencer à envoyer des messages chiffrés à cette personne. Elle, et elle seule, sera en mesure de déchiffrer et de lire vos messages, car elle est la seule personne qui dispose de la *clé privée* correspondante.

De la même façon, si vous envoyez une copie de votre propre *clé publique* à tous vos contacts et gardez la *clé privée* secrète, vous et vous seul serez en mesure de lire les messages chiffrés que vous enverrez vos contacts.

**Enigmail** vous permet également d'attacher des *signatures numériques* à vos messages. Le destinataire de votre

message qui dispose d'une copie légitime de votre clé publique pourra vérifier que le message provient bel et bien de vous, et que son contenu n'a pas été altéré en chemin. En échange, si vous avez la clé publique d'un correspondant, vous pouvez vérifier la signature numérique de ses messages.

## 4.1 Comment installer Enigmail et GnuPG

Veuillez consulter la section **Téléchargement** <sup>[127]</sup> pour obtenir les consignes de téléchargement d'**Enigmail** et de **GnuPG**.

### 4.1.1 Comment installer GnuPG

L'installation de **GnuPG** est très simple et ressemble au processus d'installation de programmes que vous avez déjà probablement déjà effectué.

Pour installer **GnuPG**, suivez les étapes énumérées ci-dessous:





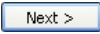
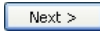
**Première étape.** Double-cliquez sur  gnupg-w32cli-1.4.11 pour lancer le processus d'installation. Il est possible que la boîte de dialogue *Fichier ouvert - Avertissement de sécurité* s'affiche. Si c'est le cas, cliquez sur  pour afficher la fenêtre suivante:



Figure 1: L'assistant d'installation de GNU Privacy Guard

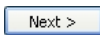
**Deuxième étape.** Cliquez sur  pour afficher la fenêtre *GNU Privacy Guard Setup - License Agreement*; après l'avoir lu, cliquez sur  pour afficher la fenêtre *GNU Privacy Guard Setup - Choose Components*.

**Troisième étape.** Cliquez sur  pour accepter les paramètres par défaut et afficher la fenêtre *GNU Privacy Guard Setup - Install Options - GnuPG Language Selection*.

**Quatrième étape.** Sélectionnez *fr-Français* dans la liste défilante, puis cliquez sur  pour afficher la fenêtre *Choose Install Location*.

**Cinquième étape.** Cliquez sur  pour accepter l'emplacement par défaut et afficher la fenêtre *Choose Start Menu Folder*.

**Sixième étape.** Cliquez sur  pour installer **GnuPG**. Lorsque ce processus est complété, la fenêtre *Installation Complete* s'affiche.

**Septième étape.** Cliquez sur , puis sur  pour finaliser l'installation du programme **GnuPG**.


### 4.1.2 Comment installer le module complémentaire Enigmail

Après avoir complété l'installation du programme **GnuPG**, il vous faut installer le module complémentaire **Enigmail**.

Pour lancer l'installation d'**Enigmail**, suivez les étapes énumérées ci-dessous:

**Première étape.** Ouvrez **Thunderbird**, puis sélectionnez **Outils > Modules complémentaires** pour afficher la fenêtre *Modules complémentaires*; le panneau *Catalogue* sera affiché par défaut.



**Deuxième étape.** Cliquez sur  pour afficher la fenêtre suivante:

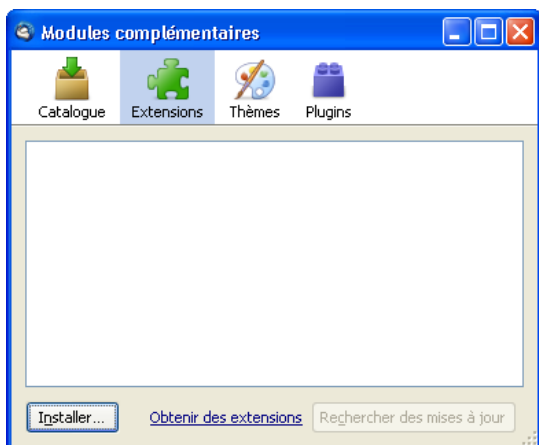


Figure 3: La fenêtre Modules complémentaires affichant le panneau Extensions

Troisième étape. Cliquez sur **Installer...** pour afficher la fenêtre suivante:

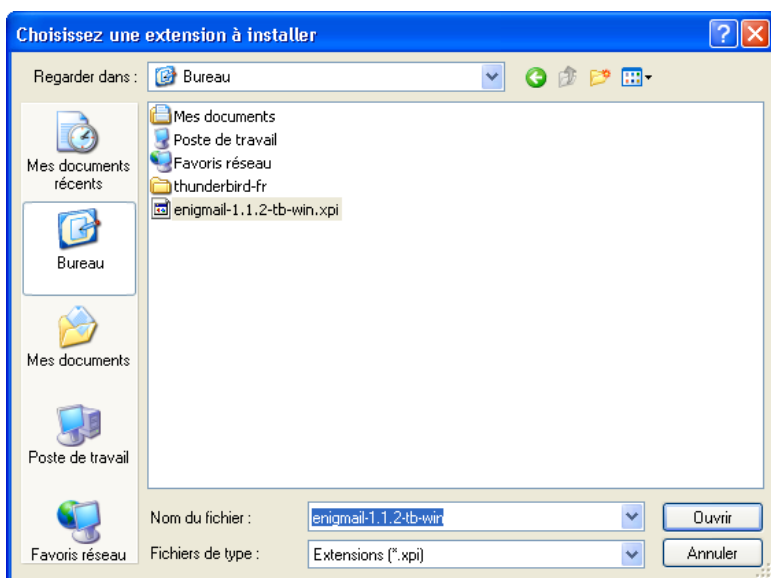


Figure 4: La fenêtre Choisissez une extension à installer

Quatrième étape. Naviguez jusqu'à l'emplacement du dossier où vous avez sauvegardé **Enigmail**, puis cliquez sur **Ouvrir** pour afficher la fenêtre suivante:

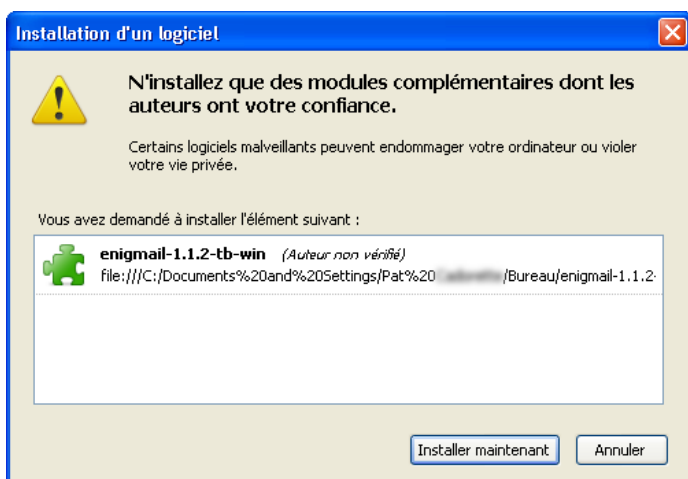


Figure 5: La fenêtre Installation d'un logiciel

**Important:** Avant de franchir cette étape, assurez-vous que vos tâches et travaux en ligne aient été sauvegardés!

Cinquième étape. Cliquez sur **Installer maintenant** pour revenir à la figure 5, puis cliquez sur **Redémarrer Thunderbird** pour finaliser l'installation du module complémentaire **Enigmail**.

Pour vérifier que l'installation d'**Enigmail** a bien été complétée, retournez à la console **Thunderbird**, et vérifiez si le bouton **OpenPGP** apparaît désormais dans la barre d'outils de **Thunderbird**.

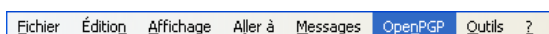


Figure 6: La barre d'outils de Thunderbird avec l'onglet OpenPGP en surbrillance

### 4.1.3 Comment confirmer qu'Enigmail et GnuPG fonctionnent normalement

Avant de commencer à utiliser **Enigmail** et **GnuPG** pour authentifier et chiffrer vos messages, vous devez d'abord vous assurer que les deux programmes communiquent normalement entre eux.

**Première étape.** Sélectionnez **OpenPGP > Préférences** pour afficher la fenêtre *Préférences OpenPGP*:

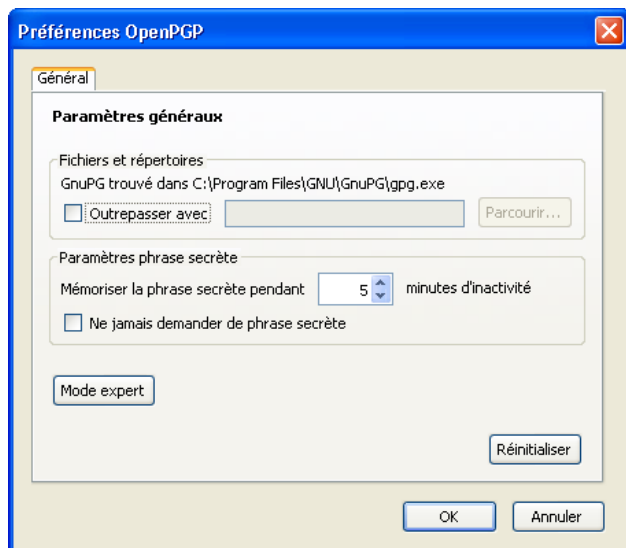


Figure 7: La fenêtre *Préférences OpenPGP*

Si **GnuPG** a été correctement installé, la ligne `GnuPG trouvé dans C:\Program Files\GNU\GnuPG\gpg.exe` sera visible dans la section *Fichiers et répertoires*; sinon il est possible que vous receviez un alerte semblable à celle-ci:

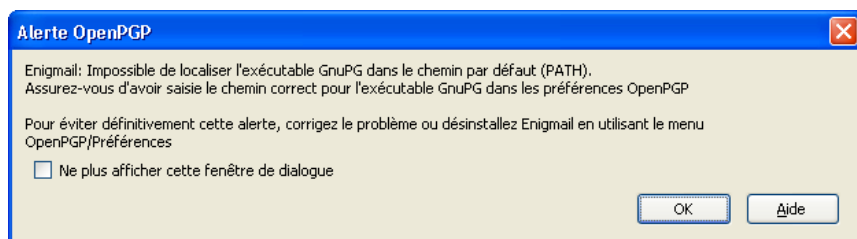


Figure 8: Exemple d'alerte *OpenPGP*

**Astuce:** Si vous avez reçu un tel message, il est possible que vous ayez installé le fichier au mauvais emplacement. Si tel est le cas, **cochez** l'option *Outrepasser avec* pour activer le bouton *Parcourir...*, **cliquez** sur *Parcourir...* pour activer la fenêtre *Localiser l'agent GnuPG* et naviguez jusqu'à l'emplacement du fichier *gpg.exe* sur votre ordinateur.

**Deuxième étape.** Cliquez sur *OK* pour retourner à la console **Thunderbird**.

## 4.2 Comment générer des paires de clés et configurer Enigmail pour qu'il fonctionne avec vos comptes de courriel

Lorsque vous avez confirmé qu'**Enigmail** et **GnuPG** fonctionnent correctement, vous être prêt à configurer un ou plusieurs de vos comptes de courrier électronique afin d'utiliser **Enigmail** pour générer une ou plusieurs paires de clés.

### 4.2.1 Comment utiliser l'assistant de configuration OpenPGP pour générer une paire de clés

**Enigmail** offre deux méthodes distinctes pour générer un paire de clés privée/publique; la première consiste à utiliser l'*Assistant de configuration OpenPGP*, et la seconde à employer la fenêtre *Gestion de clés*.

Pour générer une première paire de clés à l'aide de l'*Assistant de configuration OpenPGP*, veuillez suivre les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez **OpenPGP > Assistant de configuration** pour ouvrir la fenêtre *Assistant de configuration OpenPGP*:

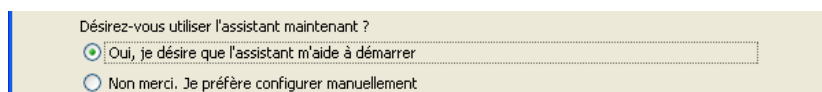


Figure 9: La fenêtre *Assistant de configuration OpenPGP - Bienvenue*

**Deuxième étape.** Cliquez sur *Suivant >* pour afficher la fenêtre suivante:

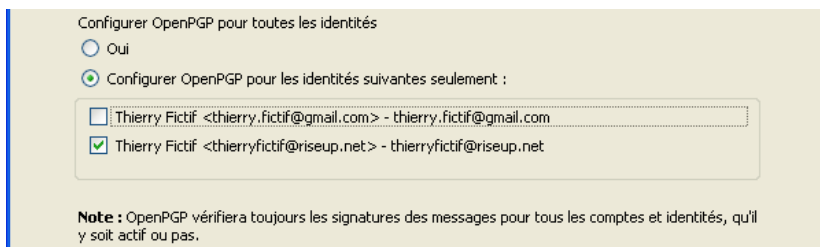


Figure 10: La fenêtre Sélectionnez une identité

Troisième étape. Cliquez sur  pour afficher la fenêtre suivante:

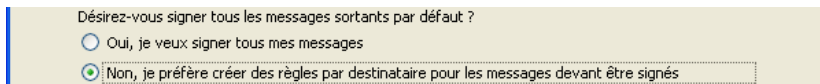


Figure 11: La fenêtre Signature - Signer numériquement vos messages sortants

Quatrième étape. Cliquez sur  pour afficher la fenêtre suivante:

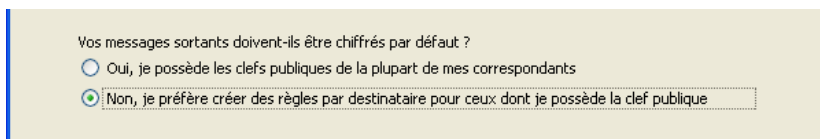


Figure 12: La fenêtre Chiffrement - Chiffrer vos messages sortants

Cinquième étape. Cliquez sur  pour afficher la fenêtre suivante:

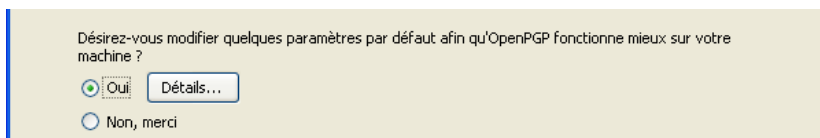


Figure 13: La fenêtre Désirez-vous modifier quelques paramètres par défaut afin qu'OpenPGP fonctionne mieux sur votre machine?

Sixième étape. Cliquez sur  pour afficher la fenêtre suivante:

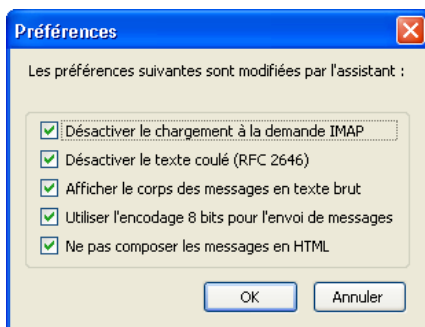


Figure 14: La fenêtre Préférences

**Commentaire:** À la section 3.2 *Comment désactiver la fonction HTML dans Thunderbird*, nous avons vu brièvement comment les messages mis en pages en HTML peuvent vous exposer à différentes menaces. Ici, les options *Afficher les corps des messages en texte brut* et *Ne pas composer les messages en HTML* servent précisément à prendre des précautions contre ces menaces.

Septième étape. Cliquez sur  pour revenir à l'Assistant de configuration OpenPGP, puis cliquez sur  pour afficher la fenêtre *Créer une clé - Créer une clé pour signer et chiffrer les messages*.

**Commentaire:** La première fois que créez une paire de clés, aucun de vos comptes de courriel n'apparaîtra dans la liste défilante.

Huitième étape. Saisissez un mot de passe complexe (ou phrase secrète) d'au moins 8 caractères alphanumériques dans les deux champs *Phrase secrète*:

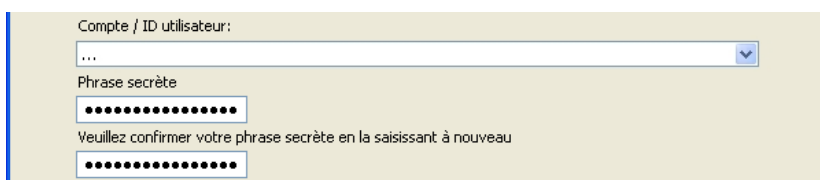


Figure 15: La fenêtre Créer une clé - Créer une clé pour signer et chiffrer les messages



**Neuvième étape.** Cliquez sur  pour confirmer ces réglages, puis cliquez sur  pour retourner à la fenêtre *Créer un clef*; le nom de votre premier compte de courriel devrait maintenant être affiché, comme suit:

Compte / ID utilisateur:  
Thierry Fictif <thierryfictif@riseup.net> - thierryfictif@riseup.net

Figure 16: Le Compte /ID utilisateur nouvellement créé

**Dixième étape.** Cliquez sur  pour afficher la fenêtre *Résumé*, qui devrait être fidèle aux réglages utilisés lors de la création de la paire de clés.

**Commentaire:** Chaque paire de clés générée avec l'*Assistant de configuration OpenPGP* est automatiquement basée sur une structure 2048-bit et a une durée de vie de 5 ans. Ces deux caractéristiques ne peuvent pas être modifiées après la création d'une paire de clés à l'aide de cette méthode.

## 4.2.2 Comment générer une paire de clés et un certificat de révocation supplémentaires pour un autre compte de courriel

Il est de pratique courante de conserver une paire de clés distincte pour chaque compte de courriel. Suivez les étapes énumérées ci-dessous pour générer des paires de clés supplémentaires pour vos autres comptes. La création d'une paire de clés implique également la création d'un *certificat de révocation* qui lui est associé. Envoyez ce certificat à vos contacts pour leur permettre de désactiver votre clé publique dans l'éventualité où votre clé privée serait compromise ou perdue.

**Première étape.** Sélectionnez **OpenPGP > Gestion de clefs** pour afficher la fenêtre suivante:

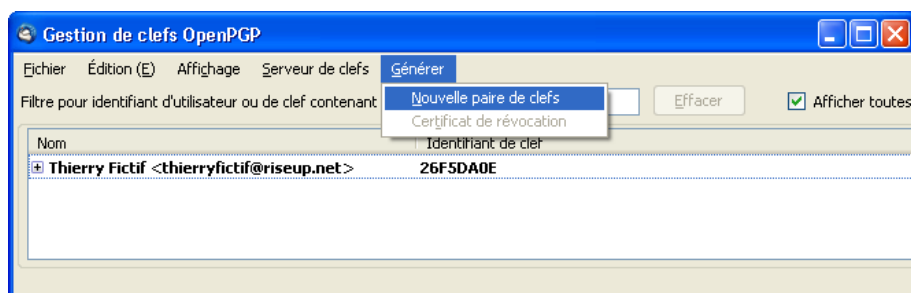


Figure 17: Le menu *Générer* du gestionnaire de clefs OpenPGP Key avec l'option *Nouvelle paire de clefs* sélectionnée

**Commentaire:** **Cochez** l'option *Afficher toutes les clefs par défaut* pour afficher la paire de clés générée à l'aide de l'*Assistant de configuration OpenPGP* pour votre premier compte de courriel, tel qu'illustré à la *figure 17* ci-dessus.

**Deuxième étape.** Sélectionnez **Générer > Nouvelle paire de clefs** dans la fenêtre de *gestion de clefs*, tel qu'illustré à la *figure 20* ci-dessus, pour afficher la fenêtre suivante:

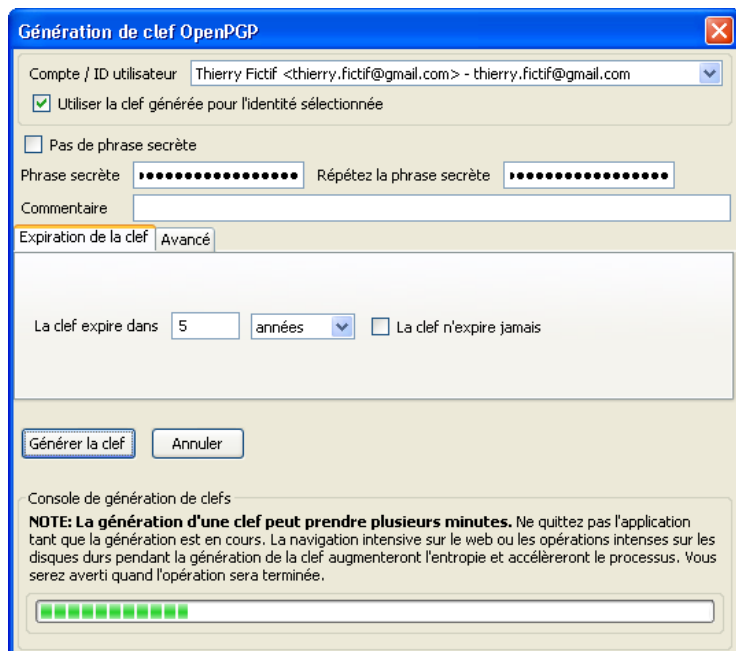


Figure 18: La fenêtre *Génération de clefs OpenPGP*

**Troisième étape.** Sélectionnez un compte de courriel électronique dans la liste défilante *Compte / ID utilisateur*, puis **cochez** l'option *Utiliser la clef générée pour l'identité sélectionnée*. Créez ensuite une phrase secrète pour protéger votre clé privée.

**Commentaire:** Comme son nom l'indique, une phrase secrète est en quelque sorte un mot de passe long et complexe. **Enigmail** vous demande de choisir un mot de passe qui est plus long et plus complexe que d'habitude.

**Important:** Il faut *toujours* générer une paire de clés avec une phrase secrète, et ne *jamais* activer l'option 'Pas de phrase secrète'.

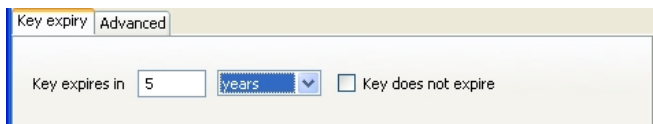


Figure 19: La fenêtre Génération de clef OpenPGP affichant l'onglet Expiration de la clef

**Commentaire:** La durée de vie d'une paire de clés dépend uniquement de vos besoins en matière de confidentialité et de sécurité. Plus vous changez fréquemment de paires de clés, plus il est difficile pour une tierce partie de compromettre votre nouvelle paire de clés. Par contre, chaque fois que vous changez de paire de clés, vous devez l'envoyer à vos correspondants et recommencer la vérification.

**Cinquième étape.** Saisissez le nombre approprié, puis sélectionnez l'unité de temps désiré (*jours, mois ou années*) pour déterminer la durée de vie de la paire de clés.

**Sixième étape.** Cliquez sur **Générer la clef** pour afficher la fenêtre suivante:

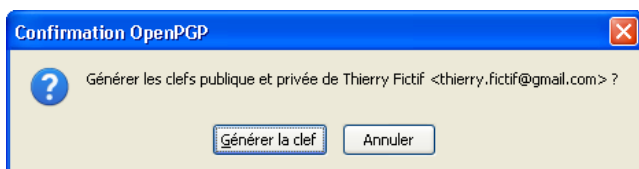


Figure 20: La boîte de dialogue de Confirmation OpenPGP

**Septième étape.** Cliquez sur **Générer la clef** pour afficher la fenêtre suivante:

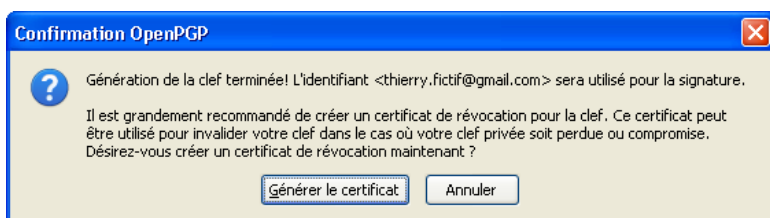


Figure 21: La boîte de dialogue de Confirmation OpenPGP

**Huitième étape.** Cliquez sur **Générer le certificat** pour afficher la fenêtre de navigation *Créer et enregistrer le certificat de révocation*.

**Commentaire:** Si vous avez connaissance qu'une tierce partie hostile ou malveillante est parvenue à accéder sans autorisation à votre clé privée, ou que vous avez vous-même perdu l'accès, vous pouvez envoyer un certificat de révocation à vos contacts pour les informer qu'ils ne doivent plus utiliser votre clé publique. Soyez aussi conscient que vous devrez mener cette opération si votre ordinateur est perdu, volé ou confisqué. Il est fortement recommandé de faire une copie de sauvegarde sécurisée de votre certificat de révocation.

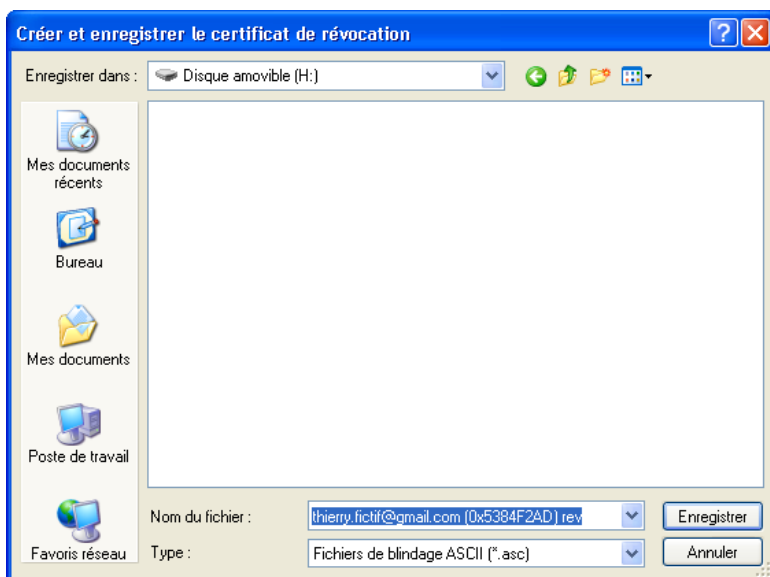


Figure 22: La fenêtre Créer et enregistrer le certificat de révocation

**Neuvième étape.** Cliquez sur **Enregistrer** pour afficher la fenêtre suivante; puis saisissez la phrase secrète associée à ce compte:

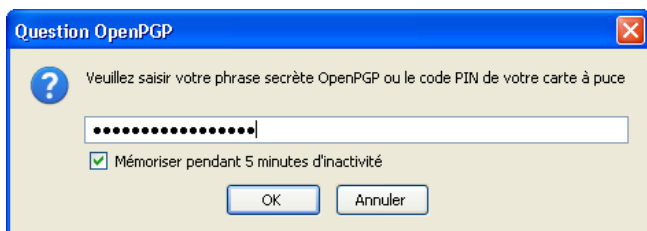


Figure 23: La fenêtre *Veillez saisir votre phrase secrète OpenPGP*

**Dixième étape.** Cliquez sur  pour finaliser la génération de la paire de clés et du certificat de révocation, et revenir à la fenêtre suivante:

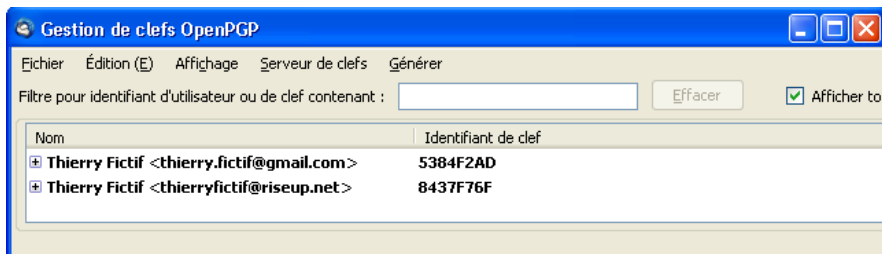


Figure 24: La fenêtre *Gestion de clefs OpenPGP* affichant la nouvelle paire de clés

**Commentaire:** Cochez l'option *Afficher toutes les clefs par défaut* pour afficher toutes les clés avec leur compte respectif, si vous êtes seul et dans un milieu sûr.

Maintenant que vous avez généré une paire de clés et un certificat de révocation, vous êtes prêt à échanger vos clés publiques avec un correspondant de confiance.

### 4.2.3 Comment configurer Enigmail pour une utilisation avec votre compte de courrier électronique

Pour activer l'utilisation d'**Enigmail** avec un compte en particulier, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez **Outils > Paramètres des comptes**.

**Deuxième étape.** Sélectionnez l'item de menu *OpenPGP* dans l'encadré de gauche, tel qu'illustré ci-dessous:

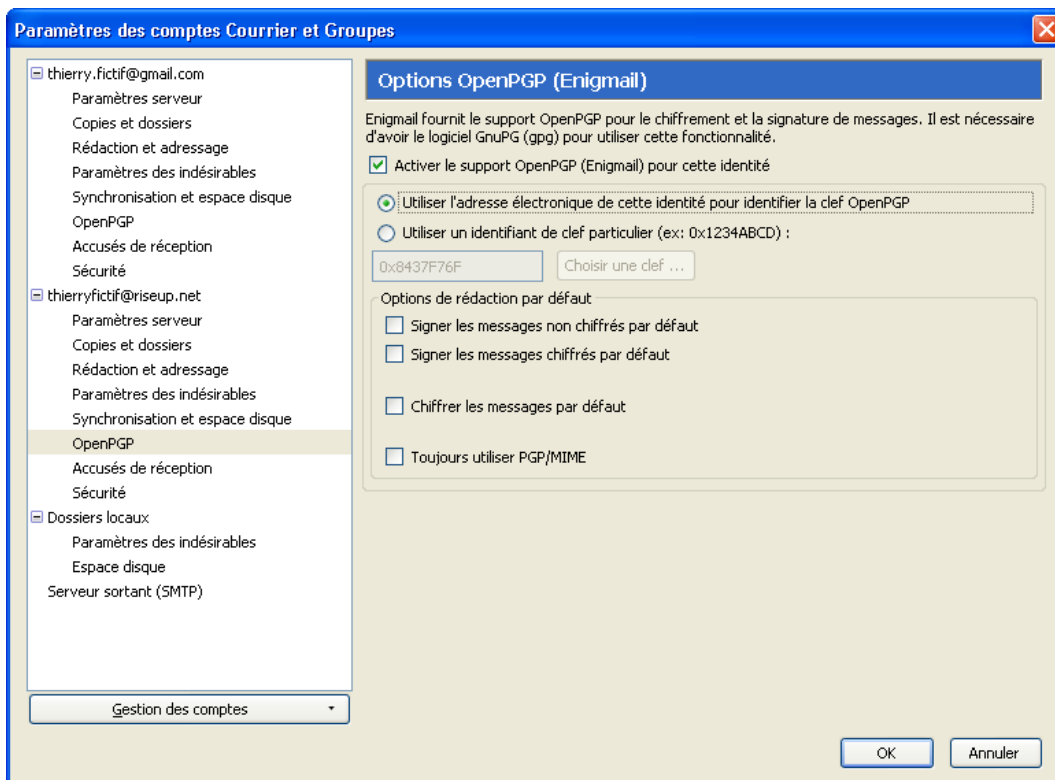


Figure 25: La fenêtre *Paramètres des comptes - OpenPGP*

**Troisième étape.** Cochez l'option *Activer le support OpenPGP (Enigmail) pour cette identité* et sélectionnez l'option *Utiliser l'adresse électronique de cette identité pour identifier la clef OpenPGP*, tel qu'illustré ci-dessus à la figure 25.


**Quatrième étape.** Cliquez sur  pour revenir à la console **Thunderbird**.

## 4.3 Comment échanger vos clés publiques

Avant de commencer à envoyer et recevoir des messages chiffrés, vous et vos correspondants devez échanger vos clés publiques. Vous devez également confirmer la validité des clés que vous acceptez en vous assurant qu'elles appartiennent bel et bien aux expéditeurs qui sont censées vous les avoir envoyées.

### 4.3.1 Comment envoyer une clé publique avec Enigmail

Pour envoyer une clé publique en utilisant **Enigmail/OpenPGP**, vous et votre correspondant devez suivre les étapes énumérées ci-dessous:

**Première étape.** Ouvrez Thunderbird, puis cliquez sur  pour rédiger un nouveau message.

**Deuxième étape.** Sélectionnez l'option de menu **OpenPGP > Attacher ma clé publique**.

**Commentaire:** Avec cette méthode, la clé ne s'affiche pas immédiatement dans le panneau **Pièces jointes**; il apparaîtra aussitôt que vous enverrez le message.

Si vous souhaitez envoyer une autre clé publique, sélectionnez l'option de menu **OpenPGP > Attacher une clé publique...** et sélectionnez la clé que vous désirez envoyer.

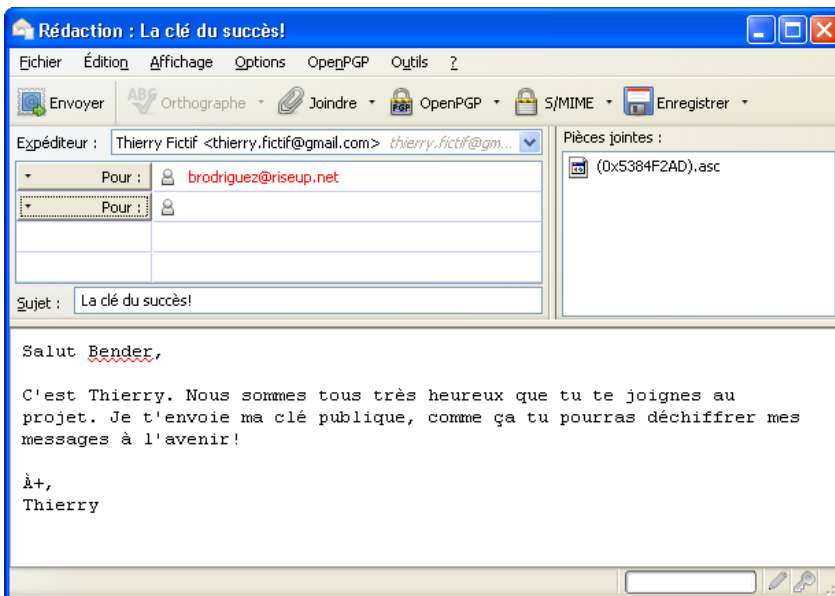



Figure 26: La fenêtre de rédaction d'un message affichant la clé publique dans le panneau des pièces jointes

**Troisième étape.** Cliquez sur  pour envoyer votre message avec votre clé publique jointe. Il est possible que la fenêtre suivante s'affiche alors:

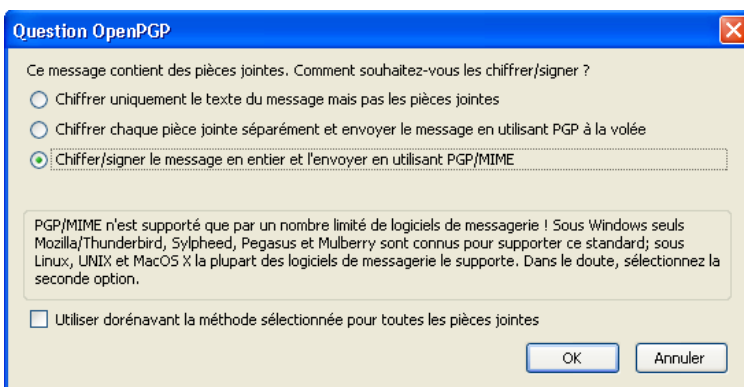



Figure 28: La fenêtre d'invite de OpenPGP servant à définir le mode de chiffrement et de signature par défaut

**Quatrième étape.** Cochez l'option *Chiffrer/signer le message en entier*, puis cliquez sur  pour afficher la fenêtre d'invite illustrée à la figure 23.


**Cinquième étape.** Saisissez votre phrase secrète, puis cliquez sur  pour afficher la fenêtre suivante:



Figure 29: La fenêtre d'invite d'OpenPGP - Do you want to encrypt the message before saving screen

**Sixième étape.** Cliquez sur **Encrypt Message** pour chiffrer, signer et envoyer votre message.

### 4.3.2 Comment importer une clé publique avec Enigmail

Vous et votre correspondant devrez suivre les étapes énumérées ci-dessous pour importer la clé publique de l'autre:

**Première étape.** Sélectionnez et ouvrez le message qui contient la clé publique de votre correspondant.

Si la clé publique de votre correspondant est incorporée au message, le bouton *Déchiffrer* sera activé et l'en-tête suivante s'affichera dans le panneau du message:

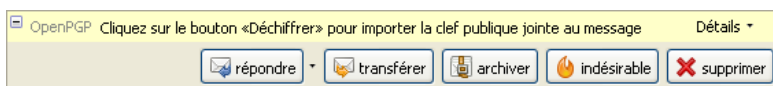


Figure 30: Le message Cliquez sur le bouton 'Déchiffrer' pour importer la clef publique jointe au message

**Deuxième étape.** Cliquez sur **Decrypt** pour lancer automatiquement le balayage du message reçu pour détecter des données chiffrées. Lorsqu'*Enigmail/OpenPGP* détecte un message contenant une clé publique, il vous demande d'importer la clé comme suit:

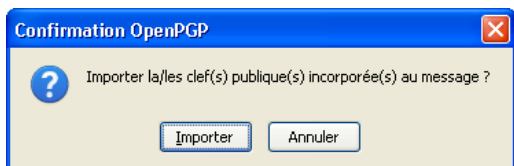


Figure 31: L'invite de confirmation OpenPGP Importer la/les clef(s) publique(s) incorporée(s) au message?

**Troisième étape.** Cliquez sur **Importer** pour importer la clé publique de votre correspondant.

Si vous avez réussi à importer la clé publique, un message semblable à celui-ci s'affichera:

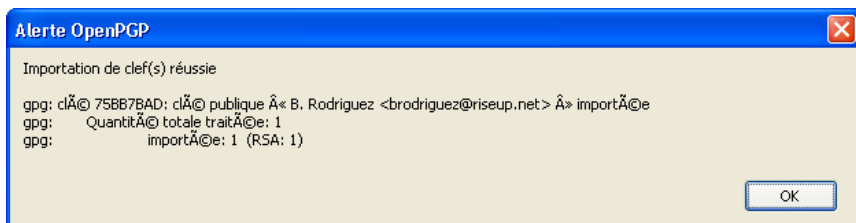


Figure 32: Une fenêtre d'alerte OpenPGP affichant la clé publique de votre correspondant

Pour confirmer que vous avez reçu la clé publique de votre correspondant, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez **OpenPGP > Gestion de clefs** pour afficher la fenêtre *Gestion de clefs OpenPGP*:

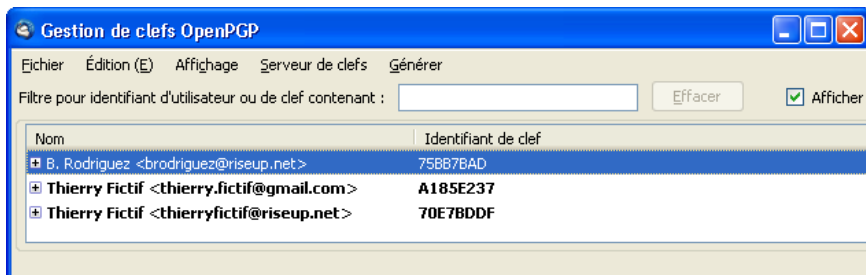


Figure 33: La fenêtre OpenPGP - Gestion de clefs affichant la clé publique récemment importée

## 4.4 Comment valider et signer un paire de clés

Finalement, vous devez vérifier que la clé importée appartient bel et bien à la personne censée vous l'avoir envoyée, et confirmer sa 'validité'. C'est une étape importante que vous et vos contacts devrez suivre pour chaque clé publique que vous recevez.

#### 4.4.1 Comment valider une paire de clés

**Première étape.** **Contactez** votre correspondant par un autre moyen de communication que le courrier électronique. Vous pouvez utiliser le téléphone, le message texte, You can use a telephone, text messages, la **Voix sur réseau IP (VoIP)** ou toute autre méthode, mais vous **devez** être absolument certain que vous communiquez avec la bonne personne. À cet égard, les conversations téléphoniques ou les rencontres en face à face sont les meilleures solutions possibles, si vous êtes en mesure de le faire.

**Deuxième étape.** Vous et votre correspondant devez vérifier l'empreinte des clés publiques que vous avez échangées. Une empreinte est une série unique de chiffres et de lettres qui sert à identifier chaque clé. Vous pouvez utiliser la fenêtre de *Gestion de clés d'OpenPGP* pour visualiser l'empreinte des paires de clés que vous avez créées et des clés publiques que vous avez importées.

Pour visualiser l'empreinte d'une paire de clés en particulier, suivez les étapes énumérées ci-dessous:

**Première étape.** **Sélectionnez > OpenPGP > Gestion de clés**, puis **cliquez à droite** sur la clé dont vous voulez vérifier l'empreinte pour afficher le menu contextuel suivant:

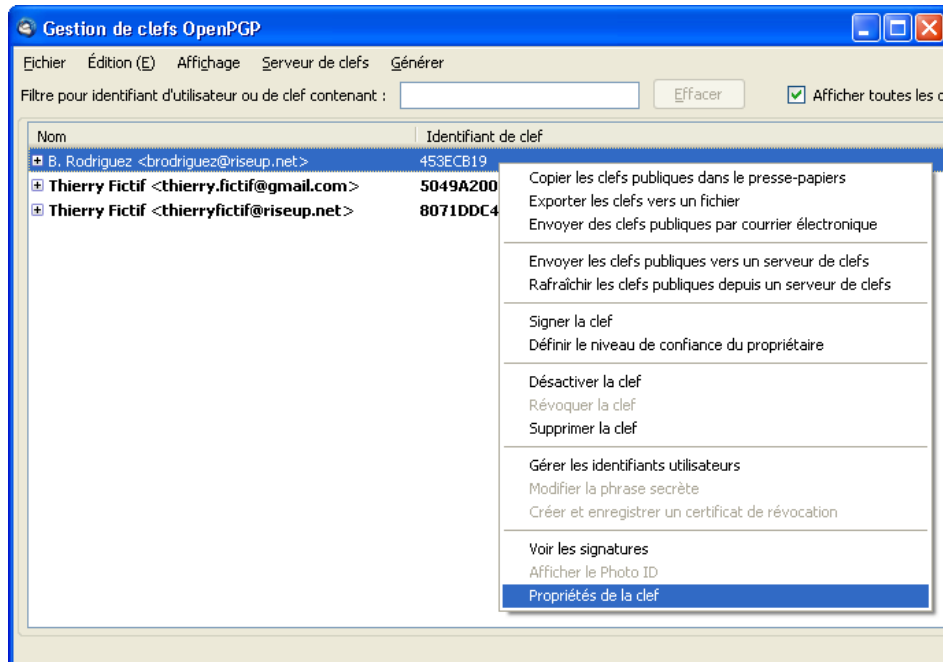


Figure 34: Le menu contextuel de *Gestion de clés d'OpenPGP* avec l'item *Propriétés de la clé* sélectionné

**Deuxième étape.** **Sélectionnez** l'item *Propriété de la clé* pour afficher la fenêtre suivante:

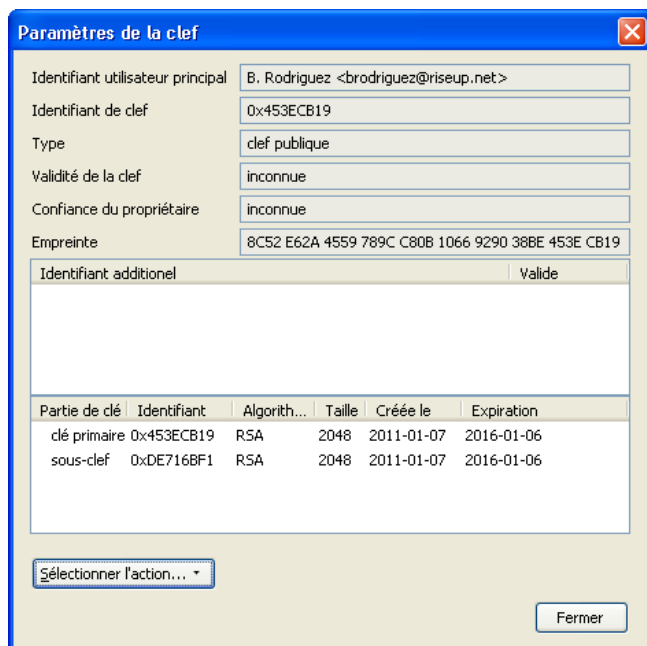


Figure 35: La fenêtre *Propriétés de la clé*

Votre correspondant devrait suivre les mêmes étapes. Confirmez l'un auprès de l'autre que l'empreinte des clés que vous avez correspond bel et bien à l'original. Si les empreintes ne correspondent pas, échangez vos clés publiques à nouveau et répétez le processus de validation.

**Commentaire:** L'empreinte elle-même n'est pas secrète et peut être enregistrée quelque part en vue d'une vérification ultérieure.

## 4.4.2 Comment signer une clé publique validée

Lorsque vous avez déterminé que la clé publique d'un correspondant donné est valide, vous devez la *signer* pour confirmer que vous considérez cette clé comme valide.

Pour signer une clé publique validée, suivez les étapes énumérées ci-dessous:

**Première étape.** Cliquez sur  pour revenir à la fenêtre *Gestion de clés*

**Deuxième étape.** Cliquez à droite sur la clé publique de votre correspondant, puis **sélectionnez** l'item *Signer la clé* dans le menu contextuel pour afficher la fenêtre suivante:

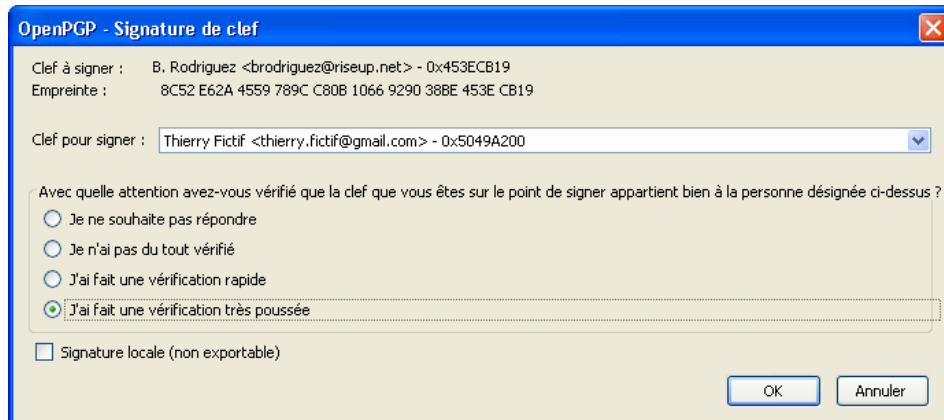



Figure 36: La fenêtre OpenPGP - Signature de la clé

**Troisième étape.** Cochez l'option *J'ai fait une vérification très poussée*, puis cliquez sur  pour compléter la signature de la clé publique de votre correspondant, finaliser le processus de validation et revenir à la fenêtre *Gestion de clés OpenPGP*:

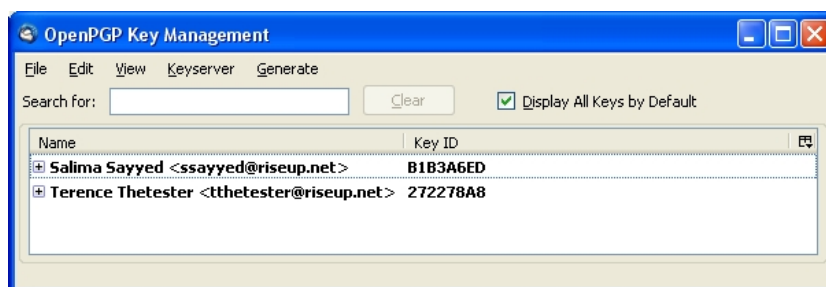


Figure 37: La fenêtre Gestion de clés OpenPGP affichant la paire de clés validée

## 4.4.3 Comment gérer vos paires de clés

La fenêtre *Gestion de clés OpenPGP* est utilisée pour générer, valider et signer différentes paires de clés. Il vous est aussi possible de mener d'autres tâches de gestion, y compris:

- **Modifier la phrase secrète:** Cette fonction vous permet de changer la phrase secrète qui protège votre paire de clés.
- **Gérer les identifiants utilisateurs:** Cette fonction vous permet d'associer plus d'un compte de courriel à une paire de clés donnée.
- **Créer et enregistrer un certificat de révocation:** Cette fonction vous permet de générer un nouveau certificat de révocation si vous avez perdu celui que vous aviez créé à l'origine.

## 4.5 Comment chiffrer et déchiffrer des messages

**Important:** L'en-tête d'un message de courrier électronique, c'est-à-dire le *Sujet* et les destinataires (y compris tous les renseignements inclus dans les champs *Pour*, *CC* et *BCC*), *ne peut pas* être chiffrée et sera envoyée en clair. Pour préserver la confidentialité et la sécurité de vos communications par courriel, le sujet ou le titre de vos messages devraient être vague et non descriptifs pour éviter de révéler des renseignements sensibles. De plus, il est fortement recommandé de mettre toutes les adresses de vos destinataires dans le champs *BCC* lorsque vous envoyez des messages à un groupe de personnes.

Lorsque vous chiffrez des messages avec des pièces jointes, il est fortement recommandé d'utiliser l'option **PGP/MIME**, puisque ceci étendra le chiffrement aux fichiers joints au message.

### 4.5.1 Comment chiffrer un message

Une fois que vous et votre correspondant avez tous deux importé, validé et signé vos clés publiques respectives, vous êtes désormais prêts à envoyer des messages chiffrés et à déchiffrer ceux que l'on vous envoie.

Pour chiffrer le contenu d'un message, suivez les étapes énumérées ci-dessous:

**Première étape.** Ouvrez votre compte de courriel et cliquez sur  pour rédiger un nouveau message.



Deuxième étape. Cliquez sur  pour afficher la fenêtre suivante:



Figure 38: La fenêtre Chiffrement OpenPGP


**Commentaire:** Si vous avez coché l'option *Chiffrer/signer le message en entier et l'envoyer en utilisant PGP/MIME* à la figure 28 tel qu'indiqué, la figure 38 ne s'affichera pas.

**Troisième étape. Cochez** les options *Signer le message* et *Chiffrer le message* tel qu'illustré à la figure 38, puis **cliquez** sur  pour finaliser la signature et le chiffrement de votre message.

**Commentaire:** Pour vérifier que votre message sera bel et bien chiffré et signé, assurez-vous que les deux icônes ci-dessous figurent dans le coin inférieur droit du panneau de message:



Figure 39: Les icônes de confirmation de la signature et du chiffrement

**Quatrième étape. Cliquez** sur  pour envoyer le message. Une fenêtre d'invite vous demande de saisir votre phrase secrète pour utiliser votre clé privée et signer le message.

#### 4.5.2 Comment déchiffrer un message

Lorsque vous recevez un message chiffré, **Enigmail/OpenPGP** tentera automatiquement de le déchiffrer sur réception ou lorsque vous souhaitez l'ouvrir. La fenêtre suivante s'affiche:

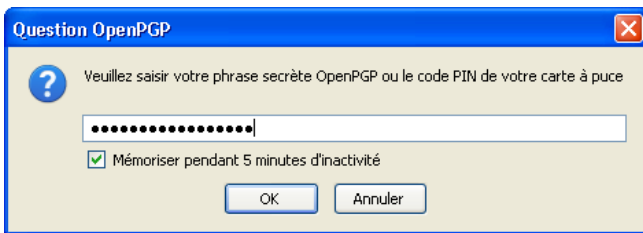


Figure 40: La fenêtre d'invite d'OpenPGP - Veuillez saisir votre phrase secrète OpnePGP ou le code PIN de votre carte à puce

**Première étape. Saisissez** votre phrase secrète tel qu'illustré à la figure 40.

Lorsque vous avez saisi la phrase secrète de votre clé privée, le message est déchiffré et affiché en clair:



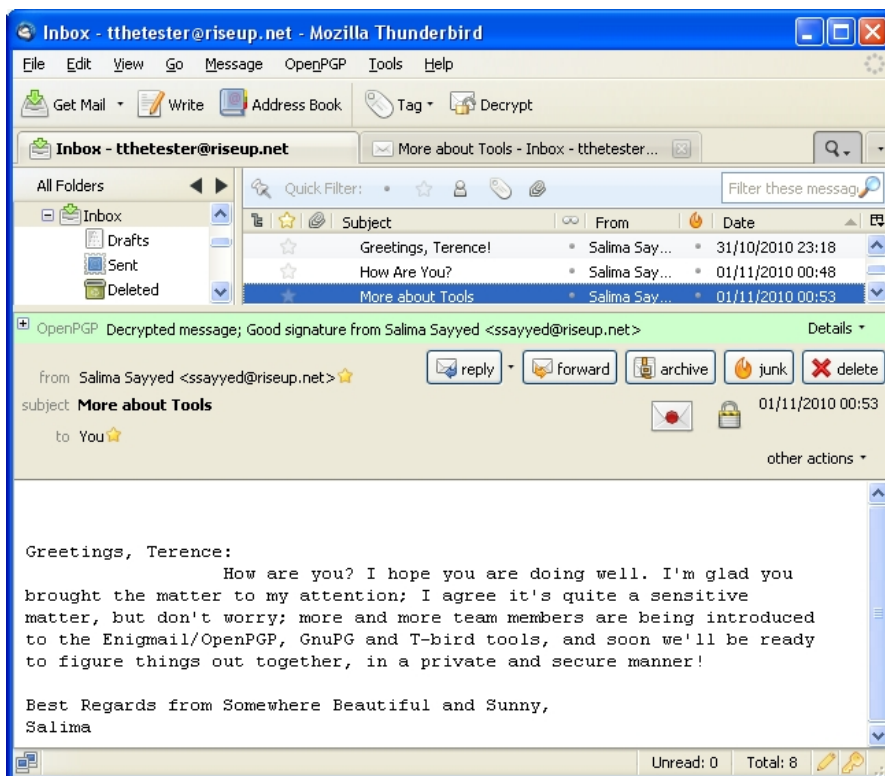


Figure 41: Le message déchiffré dans le panneau de message

Vous avez réussi à déchiffrer le message. En répétant les étapes énumérées à la section **4.5 Comment chiffrer et déchiffrer des messages** chaque fois que votre correspondant et vous échangez des messages, vous maintiendrez une voie de communication privée et sécurisée, même si des tierces parties essaient de surveiller vos communications.

## Faq et questions récapitulatives

### 5.0 Faq et questions récapitulatives

Claudia et Pablo ont configuré **Mozilla Thunderbird** pour envoyer et recevoir des messages avec leurs comptes **RiseUp**. Après avoir consulté leur courrier, ils ont été ravis de pouvoir poursuivre leur lecture des messages même après s'être déconnecté d'Internet.

Peu après, Claudia et Pablo ont installé **GnuPG** et **Enigmail**, créé leurs propres paires de clés, échangé leurs clés publiques et validé respectivement leurs clés en comparant leurs empreintes.

Même s'il leur a fallu un certain temps pour comprendre les complexités du chiffrement asymétrique (par clé publique), ils peuvent d'ores et déjà envisager les avantages que comportent un moyen de communication chiffré et sécurisé. Cependant, comme avec n'importe quel nouveau logiciel, ils ont encore quelques questions.

**Q:** *Que se passe-t-il si je n'installe qu'**Enigmail**, et pas **GnuPG**?*

**A:** *C'est simple. **Enigmail** ne fonctionnera tout simplement pas. En fait, c'est le logiciel **GnuPG** qui fournit le moteur de chiffrement utilisé par **Enigmail**.*

**Q:** *Combien de comptes de courrier électronique différents puis-je enregistrer dans **Thunderbird**?*

**A:** *Autant que tu le désires! **Thunderbird** peut facilement gérer 20 comptes de courrier électronique, ou même plus! \*\* Q: Mon ami a un compte Gmail. Devrais-je essayer de le convaincre d'installer **Thunderbird**, **Enigmail** et **GnuPG**?*

**A:** *Ce serait idéal. Il n'a qu'à s'assurer de régler ses paramètres de sécurité exactement comme tu l'as fait toi-même. Après cela, vous disposerez d'un moyen extrêmement efficace de communiquer de façon sûre et confidentielle!*

**Q:** *Rappelle-moi encore, quelle partie du message est chiffrée par **Enigmail**?*

**A:** ***Enigmail** chiffre le contenu du message. Il ne chiffre pas la ligne du sujet, ni l'adresse de courriel ou le nom que tu as choisi d'associer à ce compte de courriel. Si tu veux envoyer un message confidentiel, assure-toi que la ligne du sujet ne te trahit pas! Et si tu souhaites rester anonyme, évite d'utiliser ton vrai nom lorsque tu crées ton compte de courriel.*

**Q:** *Je ne sais toujours pas le but d'apposer une signature numérique à mes messages.*

**A:** *Une signature numérique prouve que tu es bel et bien l'expéditeur d'un message donné, et que ce message n'a pas été modifié ou piraté entre le moment où tu l'as expédié et celui où ton destinataire l'a reçu. C'est un peu comme un cachet de cire utilisé pour sceller une lettre importante.*

### 5.1 Questions récapitulatives

- Avant de pouvoir envoyer un message chiffré à un de vos collègues, quels logiciels devez-vous d'abord installer et configurer?
- Comment pouvez-vous accéder à vos messages de façon sûre en utilisant **Thunderbird**?

- Comment pouvez-vous stocker les mots de passe de vos comptes de courriel en utilisant **Thunderbird**?
- Comment pouvez-vous vous protéger contre des messages comportant du contenu malveillant?
- Quelle est la différence entre accéder à vos courriels par l'intermédiaire d'un navigateur Web, et y accéder avec un client de messagerie comme Thunderbird?

# Firefox + modules complémentaires - navigateur Internet sécurisé

## Short Description:

**Mozilla Firefox** est un navigateur Internet gratuit et de plus en plus populaire. Sa fonctionnalité est améliorée par l'inclusion de nombreux modules complémentaires, dont ceux qui augmentent le degré de confidentialité et la sécurité du navigateur lorsque vous naviguez sur le Web.

## Online Installation Instructions:

### Pour télécharger Firefox

- Lisez la courte introduction aux **Guides pratiques** <sup>[1]</sup>
- Cliquez sur l'icône **Firefox** ci-dessous pour ouvrir le site Internet [www.mozilla.org/fr/firefox/fx/](http://www.mozilla.org/fr/firefox/fx/)
- Suivez les consignes d'installation et installez **NoScript** et les autres modules complémentaires lorsque vous arrivez aux sections 4 et 5
- **Pour installer les modules complémentaires à partir du navigateur Firefox:** - Lancez Firefox - Cliquez sur les icônes ci-dessous, puis cliquez sur le bouton **Ajoutez à Firefox** sur chaque page correspondante
- Après avoir complété l'installation, vous pouvez supprimer l'exécutable d'installation du programme et des modules complémentaires

## Firefox: NoScript: Adblock Plus: Better Privacy: Beef Taco: GoogleSharing: HTTPS Everywhere:



## Site Internet

- [www.mozilla.org/fr/firefox/fx/](http://www.mozilla.org/fr/firefox/fx/) <sup>[188]</sup>

## Configuration requise

- Compatible avec toutes les versions de Windows

## Versions utilisées pour rédiger ce guide

- Firefox 10.0.2
- NoScript 2.3.2
- Adblock Plus 2.0.3
- Better Privacy 1.68
- Beef Taco 1.3.7
- GoogleSharing 0.22
- HTTPS Everywhere 2.0.1

## Licence

- FLOSS (Free/Libre Open Source Software)

**Niveau:** 1: Débutant, 2: **Moyen** 3: Intermédiaire, 4: Expérimenté, 5: Avancé

**Temps d'apprentissage:** 20 - 30 minutes

## Ce que vous apportera l'utilisation de cet outil:

- Un navigateur Web stable et sûr, dont la fonctionnalité peut être améliorée par de nombreux modules complémentaires;
- La capacité de vous protéger contre des programmes potentiellement dangereux et des sites Internet malveillants;
- La capacité d'effacer de votre ordinateur les traces de vos séances de navigation sur Internet.

## Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

Le navigateur **Mozilla Firefox** est compatible avec **GNU Linux**, **Mac OS**, **Microsoft Windows** et d'autres systèmes d'exploitation. La gestion sécurisée des pages Web est *primordiale*, puisqu'elles constituent la principale source d'infections par des programmes malveillants. C'est pourquoi nous recommandons fortement l'utilisation de **Mozilla Firefox** et des modules complémentaires proposés ici. Les bénéfices en matière de sécurité du navigateur **Firefox**, un programme multiplateforme gratuit et de source libre, sont d'autant plus remarquables lorsqu'on les compare à ses équivalents commerciaux comme **Internet Explorer**. Toutefois, si vous préférez utiliser un autre programme que **Mozilla Firefox**, nous recommandons les solutions de rechanges ci-dessous, compatibles avec **GNU Linux**, **Mac OS** et **Microsoft Windows**:

- **Google Chrome** <sup>[195]</sup>
- **Opera** <sup>[196]</sup>

## 1.1 À propos de cet outil

Dans ce guide, nous tenons pour acquis que vous savez déjà utiliser un navigateur Web; ce guide n'explique pas comment utiliser les fonctions de base du navigateur **Mozilla Firefox**. Nous y présentons plutôt quelques uns des modules

complémentaires qui contribuent à améliorer la fonctionnalité et la sécurité de **Firefox**.

Les **modules complémentaires de Mozilla Firefox** (ou "extensions"), sont des petits programmes qui ajoutent des fonctions ou améliorent les fonctions existantes de **Firefox**.

Les **Plugins de Mozilla Firefox** sont des petits logiciels habituellement conçus par des tiers partis pour permettre l'utilisation de leur programmes dans le navigateur **Firefox**.

Dans ce guide, vous apprendrez à télécharger, installer et utiliser les **modules complémentaires Mozilla** listés ci-dessous, afin d'améliorer le niveau de confidentialité et de sécurité de votre navigateur Web **Firefox** et de votre expérience de navigation en général.

Le module complémentaire **NoScript** est documenté séparément à la section **4.0 À propos de NoScript** [197]. Les autres modules complémentaires sont documentés à la section **D'autres modules utiles de Mozilla** [185]

**Important:** La très grande majorité des infections par programmes malveillants ou espions proviennent de pages Web. Il est très important de toujours évaluer s'il est sûr ou non d'ouvrir une page Web, surtout si vous l'avez reçue par courriel. Avant d'ouvrir une page Web, nous recommandons que vous en fassiez un balayage de sécurité à l'aide d'un ou l'autre des outils de balayage ci-dessous:

- [www.virustotal.com](http://www.virustotal.com) [198]
- [www.onlinelinkscan.com](http://www.onlinelinkscan.com) [199]
- [www.phishtank.com](http://www.phishtank.com) [200]

Vous pouvez également vérifier la réputation d'un site Internet en utilisant les outils ci-dessous:

- <http://safeweb.norton.com> [201]
- [www.urlvoid.com](http://www.urlvoid.com) [202]

**Offline Installation Instructions :**

**Pour installer Firefox**

- \*Lisez la courte **Introduction** aux **Guides pratiques** [1]\*\*
- **Cliquez sur l'icône Firefox ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.

**Firefox: NoScript: Adblock Plus: Better Privacy: Beef Taco: GoogleSharing: HTTPS Everywhere:**



## Comment installer et régler Firefox

Sommaire des sections de cette page:

- [2.0 À propos de Firefox](#)
- [2.1 Comment installer Firefox](#)
- [2.2 Comment régler les options du panneau Général](#)
- [2.3 Comment régler les options du panneau Vie privée](#)
- [2.4 Comment régler les options du panneau Sécurité](#)
- [2.5 Comment régler les options du panneau Avancé](#)

---

### 2.0 À propos de Firefox


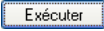
**Firefox** comporte plusieurs options faciles à régler pour protéger votre vie privée et la sécurité de votre système chaque fois que vous accédez à Internet. La fréquence à laquelle vous devrez ajuster vos réglages dépendra de votre situation particulière:

- Si vous utilisez votre ordinateur personnel et ne permettez à personne de l'utiliser pour naviguer sur Internet, vous n'aurez à configurer ces paramètres qu'une seule fois;
- Si vous êtes dans un lieu public ou au travail, vous devrez peut-être reconfigurer ces paramètres en fonction de vos besoins.

**Note:** Vous pouvez également transporter avec vous une version portable de **Firefox** sur une clé USB. Cela vous permet de configurer **Firefox** selon vos besoins et d'utiliser cette version personnalisée sur n'importe quel ordinateur public. Pour plus de renseignements à propos de **Firefox** portable, veuillez consulter le chapitre **Firefox Portable** [210].

### 2.1 Comment installer Firefox

L'installation de **Firefox** est relativement simple et rapide. Pour lancer l'installation de **Firefox**, suivez les étapes énumérées ci-dessous:

**Première étape.** Double-cliquez sur  Firefox Setup 10.0.2; si la fenêtre *Fichier ouvert - Avertissement de sécurité* s'affiche, cliquez sur  pour afficher la barre de progression *Extracting*.

Quelques instants plus tard, la fenêtre *Bienvenue dans l'assistant d'installation de Mozilla Firefox* s'affiche.

**Deuxième étape.** Suivez les étapes du processus d'installation guidé, et acceptez les options et réglages par défaut.

**Note:** Ne modifiez les options et réglages que si vous savez exactement ce que vous faites et pourquoi vous le faites.

## 2.2 Comment régler les options du panneau Général

Pour commencer à configurer **Firefox**, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez **Outils > Options...** dans la barre de menu de **Firefox**, tel qu'indiqué ci-dessous:

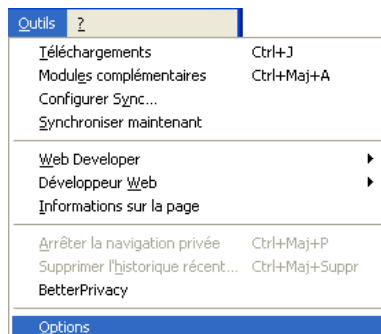


Figure 1: Le menu Outils avec l'item Options sélectionné

Cela affichera la fenêtre Options, tel qu'illustré ci-dessous:

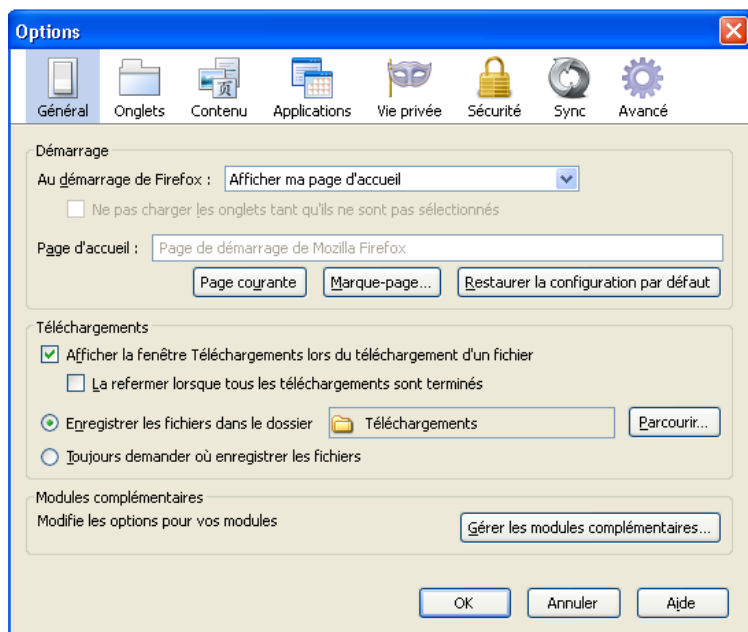


Figure 2: La fenêtre Options affichant le contenu de l'onglet Général par défaut



**Astuce:** Cliquez sur **Général** si le panneau *Général* n'est pas affichée automatiquement comme dans la Figure 2 ci-dessus.

Le panneau *Général* vous permet de régler certains fonctions de base de **Firefox**, telles que votre page d'accueil au démarrage et l'emplacement de votre dossier *Téléchargements*.

Le réglage par défaut du menu *Au démarrage de Firefox* est *Afficher ma page d'accueil*, et la page par défaut est la *Page de démarrage de Mozilla Firefox*.

**Astuce:** Cliquez sur **Page courante** pour définir une autre page de confiance comme page au démarrage.

## 2.3 Comment régler les options du panneau Vie privée

Le panneau *Vie privée* vous permet de régler les options liées à la confidentialité et la sécurité du navigateur.



**Première étape.** Cliquez sur **Vie privée** pour afficher la fenêtre suivante:

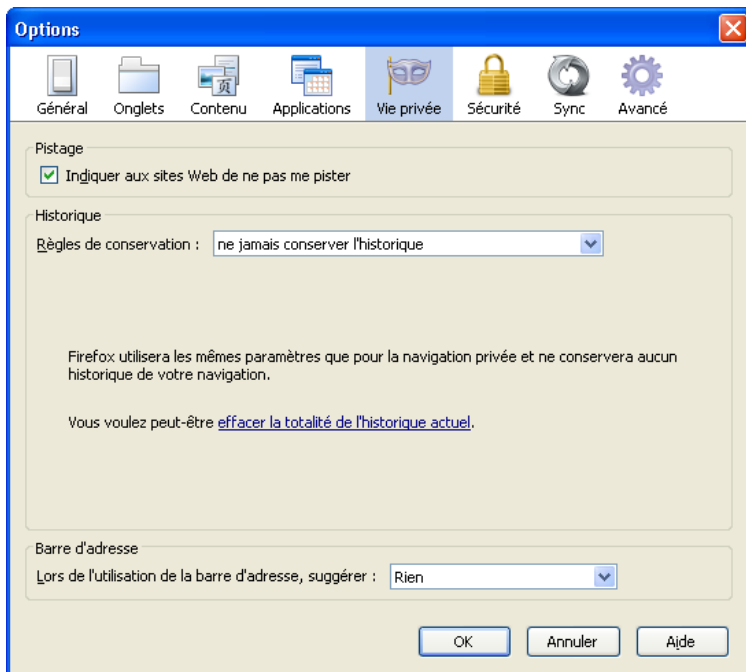


Figure 3: La fenêtre Options affichant le panneau Vie privée

Le panneau *Vie privée* est divisée en trois sections: La section *Pistage*, la section *Historique* et la section *Barre d'adresse*.

- **La section Pistage**

L'option *Indiquer aux sites Web de ne pas me pister* permet à **Firefox** d'indiquer aux sites que vous visiter de ne pas pister vos habitudes de navigation. Même si les sites Web individuels ne sont pas techniquement ou légalement forcés de respecter ces requêtes, l'activation de cette option réduit votre exposition aux publicités potentiellement dangereuses en ligne.

- **La section Historique**

Sous la rubrique *Historique*, vous pouvez gérer l'historique du navigateur **Firefox**, c.-à-d. la liste de tous les sites Internet que vous avez visités depuis que vous avez commencé à utiliser le programme. La *Règle de conservation* par défaut est *Conserver l'historique* et doit être changée pour protéger votre vie privée et votre sécurité sur Internet.

Pour supprimer les traces de votre navigation sur Internet, suivez les étapes énumérées ci-dessous:

**Première étape.** Activez la liste défilante *Règles de conservation*: et **sélectionnez** l'option *Ne jamais conserver l'historique* tel qu'illustré à la Figure 3.

**Deuxième étape.** Cliquez sur [effacer la totalité de l'historique actuel](#) pour afficher la fenêtre suivante:



Figure 4: La fenêtre Supprimer tout l'historique

**Troisième étape.** Sélectionnez toutes les cases à cocher et cliquez sur [Effacer maintenant](#) pour supprimer de **Firefox** tous les renseignements potentiellement compromettants, puis retournez au panneau *Vie privée*.

- **La section Barre d'adresse**

La section *Barre d'adresse* utilise les adresses, cookies et autres données temporaires des pages Internet marquées, et l'historique de navigation pour compléter automatiquement ou suggérer des adresses dans la barre d'**URL** de **Firefox** pour faciliter votre navigation. Le réglage par défaut de l'option *Lors de l'utilisation de la barre d'adresse, suggérer*: est *Historique et marque-pages* et doit être changé pour protéger votre vie privée et votre sécurité sur Internet.

Pour éliminer les traces de vos habitudes et historique de navigation, suivez les étapes énumérées ci-dessous:

**Première étape.** Activez la liste défilante *Lors de l'utilisation de la barre d'adresse, suggérer:* puis **sélectionnez** l'option **Rien** tel qu'illustré à la *Figure 5* ci-dessous et à la *Figure 3* ci-dessus:

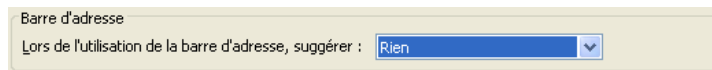


Figure 5: La section Barre d'adresse affichant l'option Rien

**Deuxième étape.** Cliquez sur  pour confirmer vos réglages et sortir de la fenêtre *Options*.

**Note:** Pour une approche plus complète de la suppression des données temporaires, veuillez consulter le chapitre portant sur **CCleaner** [211].

## 2.4 Comment régler les options du panneau Sécurité

Le panneau *Sécurité* est divisé en deux sections: la première sert à déterminer les mesures à prendre en cas d'actions potentiellement dangereuses provenant de l'extérieur, et la seconde, la section *Mots de passe*, sert à déterminer la gestion des mots de passe.

**Note:** Pour plus de renseignements sur le stockage des mots de passe, veuillez consulter le chapitre portant sur **KeePass** [82].

**Première étape.** Sélectionnez **Outils > Options...** dans la barre de menu de **Firefox** pour afficher la fenêtre *Options*, puis cliquez sur l'onglet *Sécurité* pour afficher la fenêtre suivante:

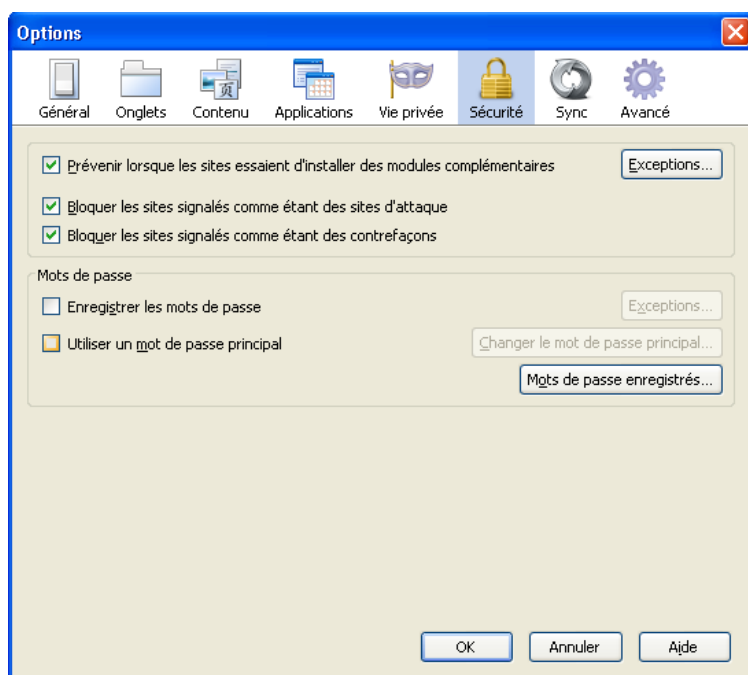


Figure 6: La fenêtre Options affichant le panneau Sécurité

**Deuxième étape.** Acceptez les réglages par défaut dans la première section.

- **La section Mots de passe**

La section *Mots de passe* vous permet de gérer vos mots de passe. L'option par défaut *Enregistrer les mots de passe* est activée la première fois que vous installez et lancez **Firefox**, et doit être désactivée pour assurer la confidentialité et la sécurité de vos mots de passe.

**Première étape.** Cliquez pour désactiver l'option *Enregistrer les mots de passe*, puis cliquez sur  pour compléter les réglages du panneau *Sécurité* dans la fenêtre *Options*.

## 2.5 Comment régler les options du panneau Avancé

L'onglet *Avancé*, comme son nom l'indique, s'adresse surtout aux utilisateurs **avancés** ou **expérimentés** de **Firefox**. Toutefois, les utilisateurs de **tous** les niveaux tireront avantage des options suivantes affichées dans l'onglet *Général*:

- L'option *Prévenir lorsque des sites Web tentent de rediriger ou de recharger la page* permet à **Firefox** d'empêcher des sites Web de rediriger automatiquement vers une autre page ou de se recharger automatiquement à votre insu ou sans votre consentement.
- L'option *Indiquer aux sites Web de ne pas me pister* permet à **Firefox** d'indiquer aux sites que vous visitez de ne pas pister vos habitudes de navigation. Même si les sites Web individuels ne sont pas techniquement ou légalement forcés de respecter ces requêtes, l'activation de cette option réduit votre exposition aux publicités potentiellement dangereuses en ligne.

**N.-B.:** Dans les versions les plus récentes de **Firefox**, l'option *Indiquer aux sites Web de ne pas me pister* a été déplacée dans le panneau *Vie privée*, sous la rubrique *Pistage* (voir la *Figure 3*, ci-dessus).

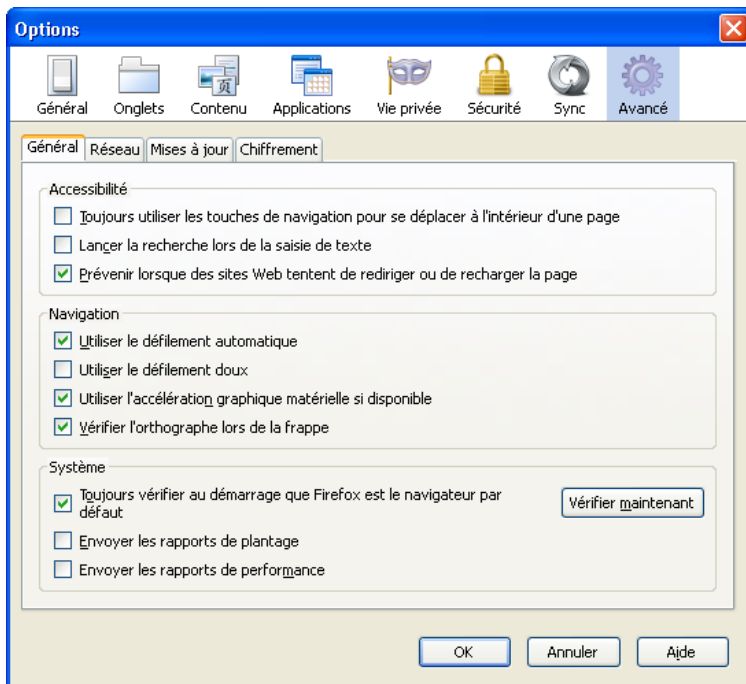


Figure 8: Le panneau d'options Avancé affichant le contenu de l'onglet Général

**Première étape.** Activez la case de l'option *Prévenir lorsque des sites Web tentent de rediriger ou de recharger la page*, tel qu'illustré à la Figure 8 ci-dessous.

**Deuxième étape.** Cliquez sur  pour enregistrer les modifications et sortir de l'onglet Avancé.

Félicitations! Firefox est maintenant réglé pour naviguer sur Internet de façon confidentielle et sécurisée.

## Comment installer des modules complémentaires Firefox

Sommaire des sections de cette page:

- [3.0 À propos des modules complémentaires de Mozilla](#)
- [3.1 Comment installer les modules complémentaires de Mozilla](#)
- [3.2 Comment désactiver ou désinstaller les modules complémentaires de Mozilla](#)
- [3.3 Comment actualiser les modules complémentaires de Mozilla](#)
- [3.4 Comment actualiser les plug-ins de Mozilla](#)

### 3.0 À propos des modules complémentaires de Mozilla

Dans le contexte des produits de **Mozilla**, un module complémentaire est en fait un programme léger qui ajoute de nouvelles fonctions ou étend la portée de fonctions existantes. En tant que tels, les modules complémentaires sont parfois appelés *extensions* et identifiés par l'extension de fichier *.xpi*. Par exemple, le fichier du module complémentaire **NoScript** est *addon-722-latest.xpi*.

Un **plugin** est essentiellement un logiciel habituellement conçu par des tiers partis pour permettre l'utilisation de leur programmes dans le navigateur **Firefox**. Un exemple bien connu est le plugin **Flash**, conçu pour afficher le contenu **Adobe Flash** dans une fenêtre de navigation de \*Firefox\*\*.

### 3.1 Comment installer les modules complémentaires de Mozilla

Le téléchargement et l'installation des **Modules complémentaires de Mozilla** est simple et rapide. Pour télécharger et installer différents modules, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez Démarrer > Mozilla Firefox ou double-cliquez sur l'icône de bureau **Firefox** pour lancer **Firefox**.

**Deuxième étape.** Saisissez <https://addons.mozilla.org/fr/firefox/> <sup>[212]</sup> dans la barre d'adresse de **Firefox** pour accéder au site des **Modules complémentaires de Mozilla pour Firefox**.

**Troisième étape.** Saisissez le nom du module complémentaire voulu dans la zone recherche de **Mozilla** (dans cet exemple, le module complémentaire **Adblock Plus**) comme ci-dessous:



Figure 1: La barre de recherche de modules complémentaires de Mozilla Firefox affichant une recherche pour Adblock Plus

Quatrième étape. Cliquez sur  ou tapez **Enter** pour afficher la fenêtre suivante:



Figure 2: Résultats de recherche pour Adblock Plus

Cinquième étape. Cliquez sur  pour afficher les fenêtre suivantes:

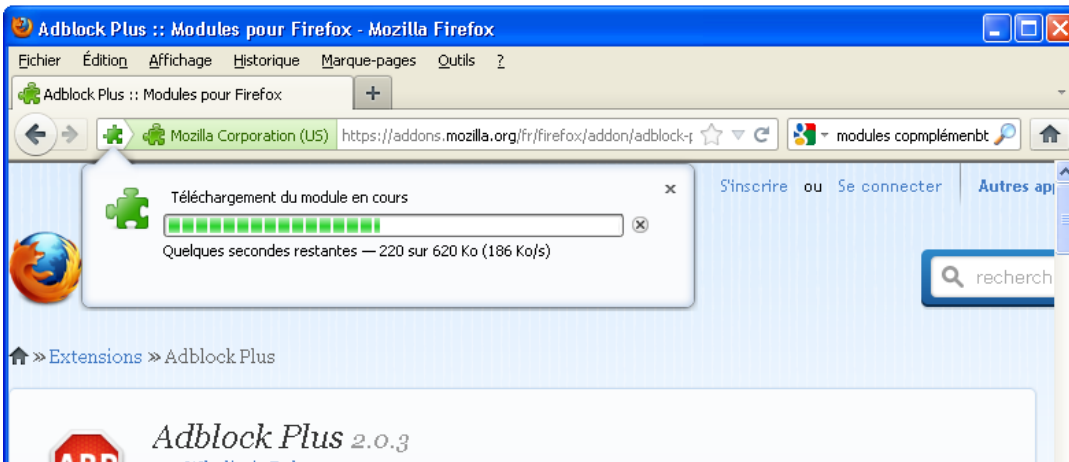


Figure 3: La fenêtre Résultats de recherche Adblock Plus :: Modules pour Firefox

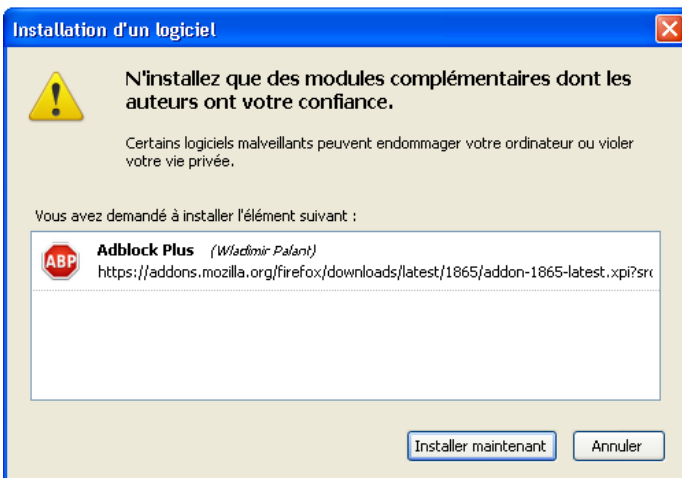



Figure 4: La fenêtre d'installation d'un logiciel associée à Adblock Plus

Sixième étape. Cliquez sur  lorsque le lien est activé pour lancer l'installation du module; lorsque l'installation est terminée, la fenêtre suivante s'affiche:

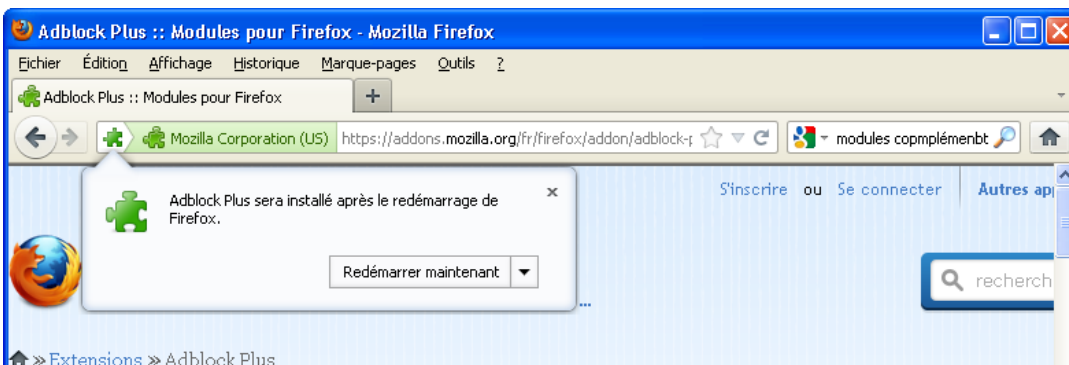


Figure 5: La fenêtre Résultats de recherche Adblock Plus :: Modules pour Firefox

Septième étape. Cliquez sur  pour compléter le processus d'installation.



Firefox redémarrera automatiquement.

**Astuce:** Cliquez sur  pour sélectionner l'option *Plus tard* si vous préférez redémarrer **Firefox** plus tard.

**Huitième étape.** Sélectionnez l'item de menu *Modules complémentaires* dans le menu *Outils* de la barre de menu de **Firefox**, pour afficher la fenêtre suivante:

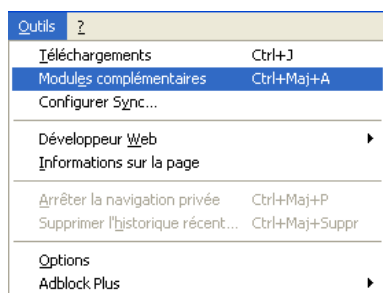


Figure 6: Le menu *Outils* avec l'item *Modules complémentaires* sélectionnés

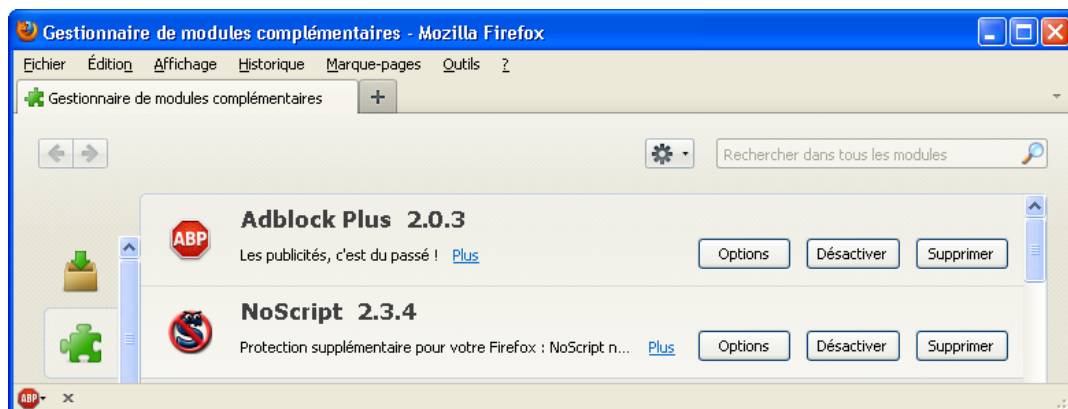




Figure 7: Le *Gestionnaire de modules complémentaires* affichant le module *Adblock Plus* nouvellement installé


**Important:** N'installez pas de modules complémentaires provenant de sources inconnues. Par souci de sécurité, n'installez que des modules complémentaires téléchargés à partir du site Internet <https://addons.mozilla.org/fr/firefox/>.

## 3.2 Comment désactiver ou désinstaller les modules complémentaires de Mozilla

L'onglet *Modules complémentaires* affiche tous les modules déjà installés, tel qu'illustré à la Figure 7. Tous les modules complémentaires de **Mozilla** peuvent être désactivés temporairement en cliquant sur , ou complètement supprimé cliquant . Toutefois, dans les deux cas, **Firefox** doit être redémarré pour que les changements soient enregistrés.

## 3.3 Comment actualiser les modules complémentaires de Mozilla

De temps à autres, les divers modules complémentaires doivent être actualisés pour rester compatibles avec la plus récente version de **Firefox**. Selon la disponibilité de votre bande passante, vous pouvez choisir d'actualiser vos modules complémentaires automatiquement ou manuellement.

**Première étape.** Cliquez sur  pour afficher le menu associé, puis sélectionnez l'item *Rechercher des mises à jour* pour actualiser manuellement vos modules complémentaires, tel qu'illustré à la Figure 8 ci-dessous.

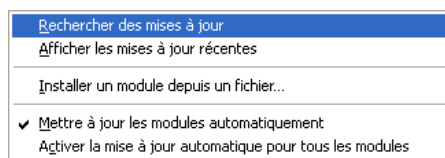


Figure 8: Le bouton d'actualisation du *Gestionnaire de modules complémentaires* affichant sa liste défilante

**Deuxième étape.** Vous pouvez également sélectionner l'option *Mettre à jour les modules automatiquement* pour actualiser vos modules automatiquement, tel qu'illustré à la Figure 8 ci-dessus.

## 3.4 Comment actualiser les plugins de Mozilla

Puisque certains plugins ne s'actualisent pas automatiquement, il est fortement recommandé de rechercher les plus récentes mises à jour des **Plugins Mozilla**.

**Important:** Il est *absolument essentiel* de faire des mises à jour au moins **une fois par mois**. Les plugins sont constamment améliorés et actualisés pour répondre à toutes sortes de problèmes de sécurité.

Pour rechercher des mises à jour de plugins manuellement, **cliquez** sur le lien suivant <https://www.mozilla.com/fr/plugincheck> [213] pour afficher le site suivant:

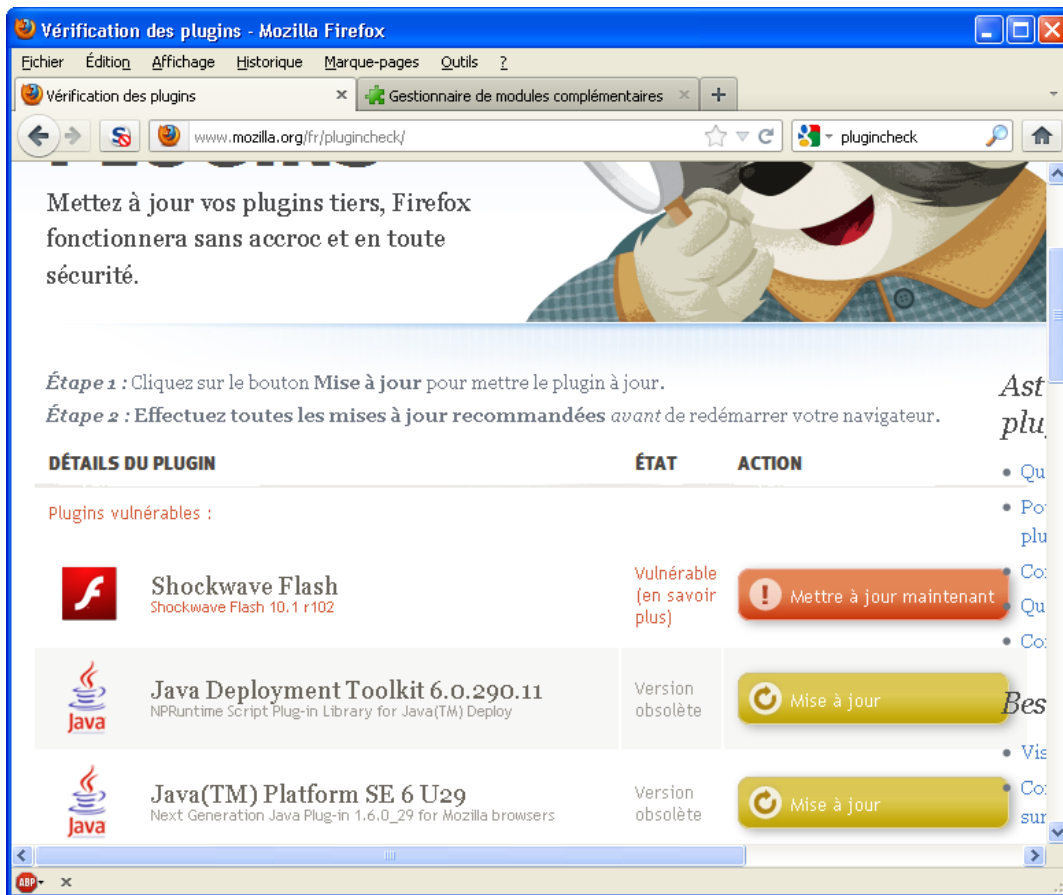


Figure 9: Le site Internet de vérification des plugins Mozilla Firefox

**Actualisez tous les plugins qui ne sont pas à jour** en cliquant sur les boutons d'action correspondants et en suivant les consignes qui s'affichent à l'écran.

Pour désactiver un plugin inconnu ou dont vous n'avez plus besoin, suivez les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez **Outils > Modules complémentaires** dans la barre de menu de **Firefox** pour afficher le *Gestionnaire des modules complémentaires*.

**Deuxième étape.** Cliquez sur l'onglet *Plugins* pour afficher la liste complète des plugins **Mozilla Firefox** installés, trouvez le plugin que vous souhaitez désactiver, puis **cliquez** sur .

## Comment utiliser le module complémentaire NoScript

Sommaire des sections de cette page:

- [4.0 À propos de NoScript](#)
- [4.1 Comment utiliser NoScript](#)
- [4.2 À propos du Clickjacking et des attaques XXS \(Cross-Site Scripting\)](#)



**NoScript** est un **module complémentaire Mozilla** particulièrement utile. Ce programme peut contribuer à protéger votre ordinateur contre des sites Internet malveillants. Il fonctionne en dressant une "liste blanche" des sites que vous avez désignés comme acceptables, sûrs ou fiables (tel qu'un site de "télébanque" à domicile ou un journal électronique). Tous les autres sites sont considérés comme potentiellement dangereux et leurs fonctions sont limitées jusqu'à ce que vous décidiez que le contenu du site ne comporte aucun risque et que vous l'ajoutiez à la liste blanche.

**NoScript** commencera à bloquer automatiquement les bannières publicitaires, les publicités intempestives (*pop-up*), **JavaScript** et les codes **Java** associés, ainsi que plusieurs autres éléments Web potentiellement dommageables. **NoScript** ne fait pas lui-même la différence entre des contenus dommageables et des contenus nécessaires à l'affichage normal des sites Internet. Il vous revient de définir des exceptions pour les sites dont vous jugez les contenus sûrs.

### 4.1 Comment utiliser NoScript

Avant de commencer à utiliser **NoScript**, assurez-vous d'avoir installé le programme correctement en **sélectionnant**

Outils > Modules complémentaires pour afficher la fenêtre des *Modules complémentaires* et confirmer l'installation.

**Astuce:** Bien que l'utilisation de **NoScript** puisse paraître laborieuse au début, (parce que, par exemple, les sites Web que vous avez l'habitude de visiter ne s'affichent pas correctement), vous tirerez immédiatement avantage de la fonction de blocage automatique des éléments suspects.

Cela bloquera toutes les publicités et fenêtres intempestives, ainsi que les éléments de code malveillants intégrés (ou piratés) à certains sites Web.

**NoScript** fonctionnera silencieusement en arrière-plan jusqu'à ce qu'il détecte la présence de contenu **JavaScript**, **Adobe Flash** ou autre contenu de type script. À ce moment-là, **NoScript** bloquera ledit contenu et la barre d'état du logiciel s'affichera au bas de la fenêtre **Firefox**, tel qu'illustré ci-dessous:

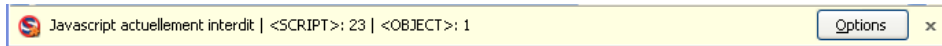


Figure 1: La barre d'état de NoScript

La barre d'état de **NoScript** affiche de l'information sur les *objets* (par exemple, la publicité et les fenêtres intempestives) et les *scripts* dont l'exécution est actuellement bloquée par le programme. Les deux figures suivantes sont des exemples typiques de **NoScript** à l'oeuvre: à la Figure 2, **NoScript** a réussi à bloquer une publicité créée en **Adobe Flash Player** sur un site commercial.



Figure 2: Un exemple de publicité intempestive bloquée par NoScript sur un site commercial

À la Figure 3, le site Internet de **Twitter** affiche un avertissement vous invitant à activer **JavaScript** (au moins temporairement) pour afficher normalement le contenu du site.

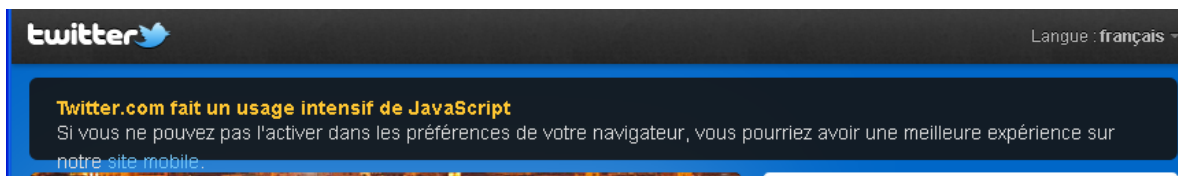


Figure 3: Le site Internet de Twitter suggère d'activer JavaScript

Puisque **NoScript** ne fait pas la différence entre code malveillant et code légitime, il est possible que certaines fonctions et fonctionnalités importantes (par exemple, une barre d'outil) soient désactivées. Certaines pages Web affichent du contenu, y compris du contenu script, provenant de plusieurs sites Internet à la fois. Par exemple, un site Internet comme **www.youtube.com** comporte trois différentes sources de scripts:

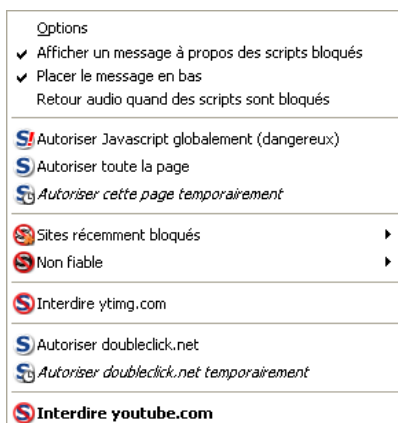


Figure 4: Un exemple d'affichage du menu de la barre d'état NoScript

Pour débloquer des scripts dans une telle situation, commencer par **sélectionner** l'option *Autoriser [cette page] temporairement* (dans ce cas-ci, youtube.com). Si cela ne vous permet pas d'afficher la page normalement, il vous faudra peut-être déterminer, par un processus d'essais et erreurs, le nombre minimal de sites nécessaire pour afficher le contenu de votre choix. Pour **YouTube**, vous n'avez qu'à **sélectionner** l'option *Autoriser youtube.com temporairement* et *Autoriser*

yiming.com temporairement pour faire en sorte que YouTube fonctionne.

**Attention!** Vous ne devriez en aucune circonstance sélectionner l'option: *Autoriser les scripts globalement (dangereux)*. Autant que possible, évitez de sélectionner l'option *Autoriser toute la page*. De temps en temps, il vous faudra peut-être autoriser tous les scripts; si une telle situation se présente, assurez-vous de le faire uniquement pour les sites dont vous avez entièrement confiance, et temporairement, c-à-d. jusqu'à la fin de votre session de navigation. Une seule injection de code malveillant suffit à compromettre votre sécurité et votre confidentialité en ligne.

## 4.2 À propos du Clickjacking et des attaques XXS (Cross-Site Scripting)

NoScript peut être configuré pour défendre votre système contre les attaques XXS (Cross-Site Scripting) et de détournement de clic (Clickjacking).

Un script *cross-site* est un type de faille de sécurité informatique qui permet à des pirates et autres intrus d'injecter un code malveillant dans une page Web existante. Un détournement de clic (ou *clickjacking*) se produit, par exemple, lorsque vous cliquez sur un bouton qui sert en apparence à accomplir une fonction quelconque, mais que le même bouton lance l'exécution d'un code ou d'un script à votre insu. Ces deux types d'attaques peuvent se produire sans que vous ne vous en rendiez compte, à moins que NoScript soit configuré pour les bloquer.

Chaque fois qu'une attaque de *clickjacking* est en cours, une fenêtre comme celle-ci apparaît:

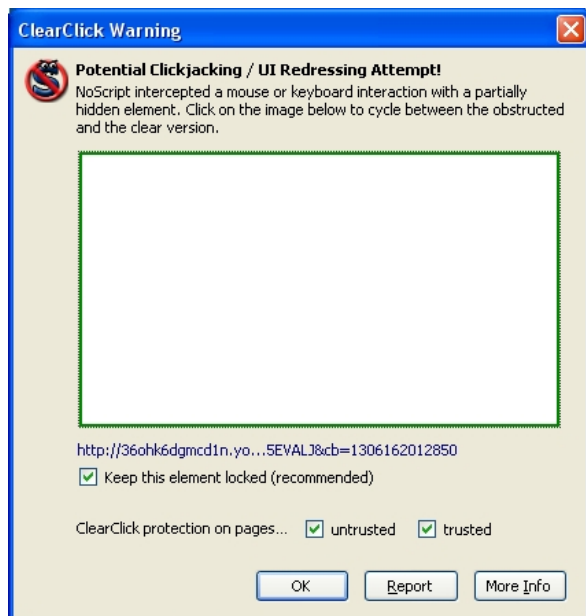


Figure 5: Un exemple de tentative d'attaque de détournement

Suivez les consignes affichées dans la fenêtre pour neutraliser la tentative de détournement, puis **cliquez** sur .

## D'autres modules complémentaires utiles de Firefox

Sommaire des sections de cette page:

- [5.0 À propos des modules complémentaires](#)
- [5.1 Comment utiliser Adblock Plus](#)
- [5.2 Comment utiliser Better Privacy](#)
- [5.3 Comment utiliser Beef Taco \(Targeted Advertising Cookies Opt-Out\)](#)
- [5.4 Comment utiliser GoogleSharing](#)
- [5.5 Comment utiliser Use HTTPS Everywhere](#)

---

## 5.0 À propos des modules complémentaires

Les **Modules complémentaires de Mozilla Firefox** présentés dans cette section servent à protéger la confidentialité, l'anonymat et la sécurité de vos sessions de navigation sur Internet. Pour les télécharger, veuillez consulter la section [Pour télécharger Firefox](#) [28].

### 5.1 Comment utiliser Adblock Plus



**Adblock Plus** est un module de filtrage de contenu conçu pour limiter ou restreindre la capacité des publicités à s'afficher. Lorsque le module **Adblock Plus** est correctement installé:

**Première étape.** Sélectionnez **Outils > Modules complémentaires** pour afficher la page des modules complémentaires. Cliquez sur l'onglet *Extensions*, puis **cliquez** sur le bouton *Options* du module **Adblock Plus**, pour afficher la fenêtre suivante.

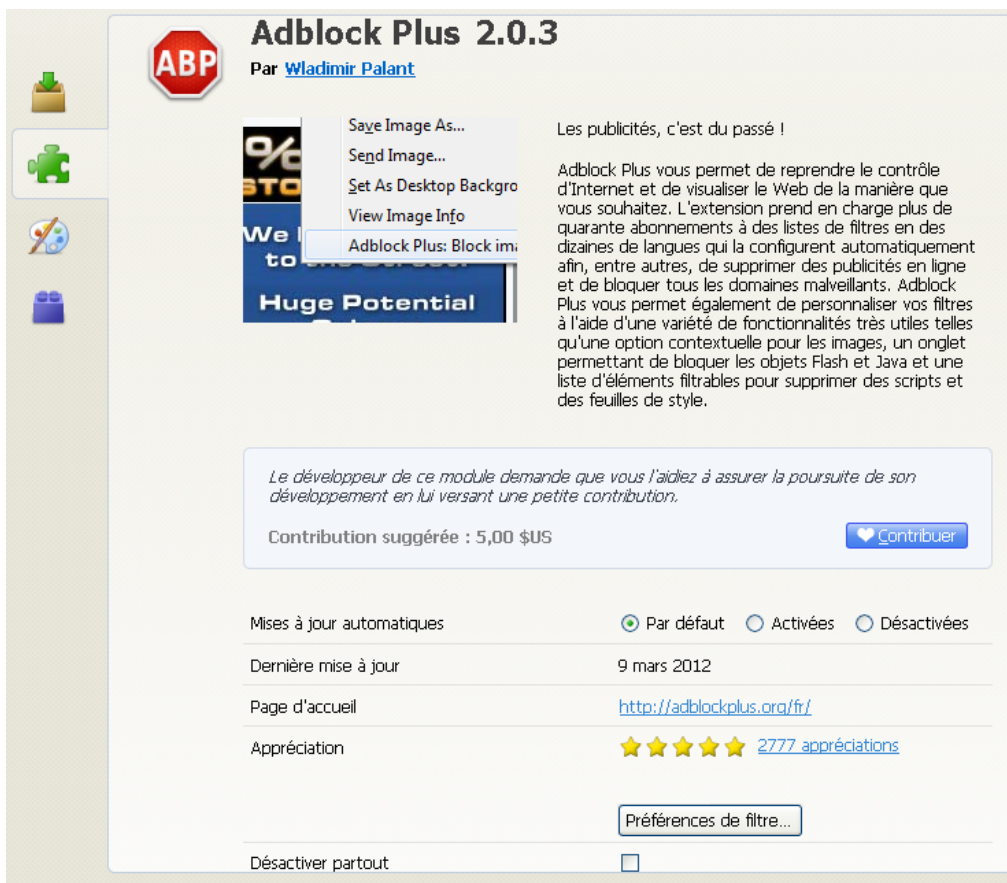


Figure 1: La fenêtre du module complémentaire Adblock Plus

Deuxième étape. Cliquez sur **Préférences de filtre...** pour afficher la fenêtre des préférences **Adblock Plus**, illustrée ci-dessous:

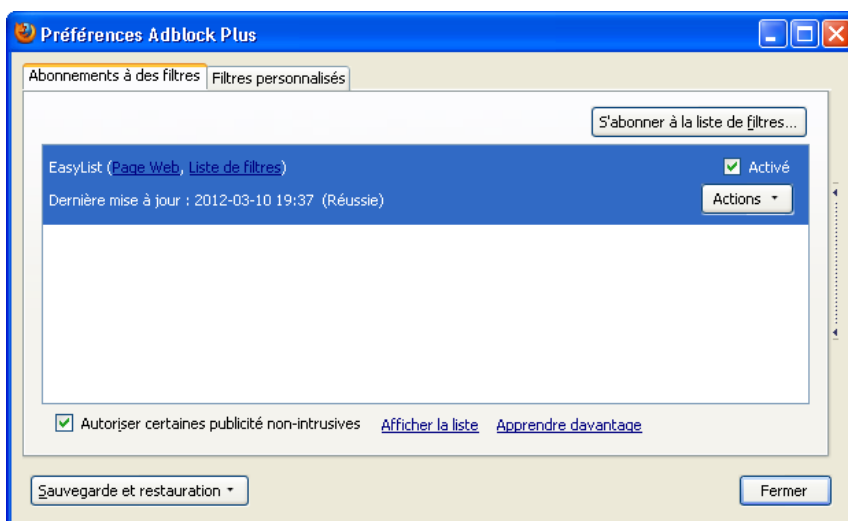


Figure 2: La fenêtre Préférences Adblock Plus

Troisième étape \*\*. \*\*Cliquez sur **S'abonner à la liste de filtres...** pour afficher la liste défilante des listes **Adblock Plus**, illustrée ci-dessous:

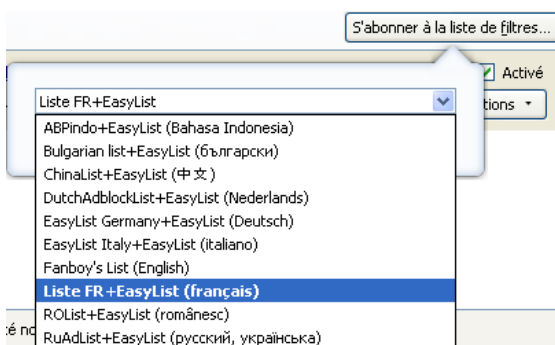



Figure 3: La liste défilante des listes Adblock Plus

Quatrième étape \*\*. **Sélectionnez** un abonnement, par exemple, la *Liste FR+EasyList (français)*, tel qu'illustré à la Figure 3 ci-dessus, puis **cliquez** sur  pour vous abonner à cette liste de filtres. À partir de maintenant, les publicités définies dans cette liste de filtres ne pourront plus s'afficher.

## 5.2 Comment utiliser Better Privacy



**Better Privacy** est un **Module complémentaire Mozilla Firefox** qui aide à protéger votre système contre un type particulier de cookie, appelé **LSO (Local Shared Objects)**, qui peut être introduit dans votre ordinateur à l'aide d'un script **Flash**. Ce type de cookie ne peut pas être éliminé par la procédure normale de suppression des cookies de **Firefox**.

## 5.3 Comment utiliser Beef Taco (Targeted Advertising Cookies Opt-Out)




**Beef Taco** est un **Module complémentaire Mozilla Firefox** qui vous permet de gérer les cookies associés aux publicités provenant de diverses entreprises, y compris **Google, Microsoft et Yahoo**. Ce module peut être configuré pour supprimer automatiquement les cookies connus sous le nom de **Targeted Advertising Cookies Opt-Out**. Les utilisateurs **expérimentés** et **avancés** peuvent également déterminer avec plus de précision quels cookies sont admis dans votre système et lesquels doivent être éliminés.

## 5.4 Comment utiliser GoogleSharing



**GoogleSharing** est un système d'anonymisation par proxy qui mélange les diverses requêtes de recherche effectuées par plusieurs utilisateurs, de telle sorte que **Google** soit incapable de déterminer *quelle* requête provient de *qui*. **GoogleSharing** est capable d'empêcher **Google** de recueillir des renseignements sur vous à partir des services qui n'exigent pas un nom d'utilisateur et un mot de passe. En général, le trafic qui n'est pas spécifiquement associé à **Google** n'est pas affecté ou redirigé.

Lorsque **GoogleSharing** est installé correctement, un bouton apparaît dans le coin inférieur droit de la barre des modules complémentaires de **Firefox**, comme suit: 

**GoogleSharing** fonctionne silencieusement en arrière-plan et n'exige aucun réglage particulier. Comme pour plusieurs options de confidentialité et de sécurité, il faut faire un compromis entre l'efficacité et la vitesse, d'une part, et une meilleure confidentialité et sécurité, d'autre part. Si vous êtes dans une situation où la vitesse est plus importante que la confidentialité, vous n'avez qu'à **cliquer** sur le bouton pour désactiver rapidement **GoogleSharing**, comme suit:



## 5.5 Comment utiliser HTTPS Everywhere



**HTTPS Everywhere** est un **Module complémentaire Mozilla Firefox** qui vous assure de toujours communiquer avec certains sites Internet particuliers de façon chiffré (protocole (*https*)). Plusieurs sites qui permettent une connexion *https* fonctionnent par défaut avec une adresse *http* non sécurisée.

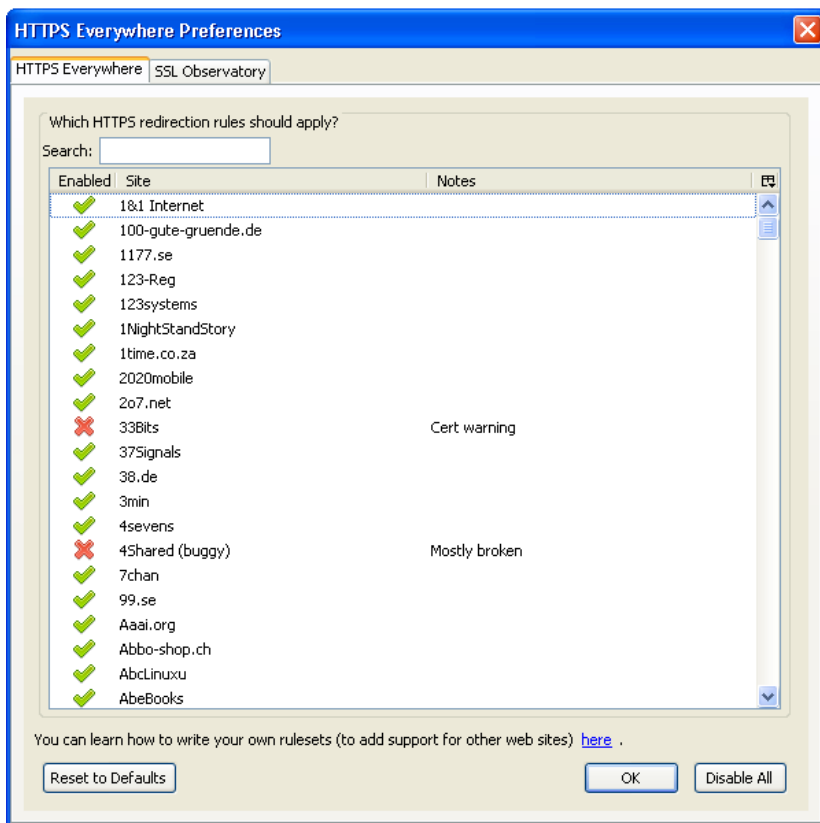


Figure 4: La fenêtre Préférences de HTTPS Everywhere

Le module **HTTPS Everywhere** remédie à ces problèmes en ré-écrivant toutes vos requêtes à ces sites avec le protocole **HTTPS**. Le programme fonctionne silencieusement en arrière-plan et vous assure que votre navigation sur les sites sélectionnés demeure sûre et sécurisée.

## Faq et questions récapitulatives

### 6.0 FAQ et questions récapitulatives

Muhindo et Salima comprennent très bien l'utilité de certains des **Modules complémentaire Firefox** recommandés, mais d'autres leur paraissent un peu plus compliqués. Heureusement, Assani est là pour aider à expliquer ces modules plus complexes.

**Q:** Pourquoi ai-je besoin d'un si grand nombre de modules complémentaires pour me défendre contre les sites Internet malveillants? Si **NoScript** me protège contre les scripts potentiellement dangereux, pourquoi ai-je en plus d'autres modules qui fonctionnent de la façon similaire?

**A:** Il est souvent judicieux d'utiliser plus d'un outil pour se prémunir contre une même menace. (Les logiciels antivirus sont une exception notable à cette règle, puisqu'ils entrent habituellement en conflit les uns avec les autres.) Ces modules complémentaires de **Firefox** emploient des techniques différentes pour protéger ton navigateur contre diverses menaces. **NoScript**, par exemple, bloque tous les scripts des sites Internet inconnus, mais la plupart des internautes ont tendance à approuver les sites qu'ils visitent régulièrement, ce qui ouvre la porte à des scripts potentiellement malveillants. Les utilisateurs de **NoScript** ont aussi tendance à permettre aux sites inconnus de charger leurs scripts, de façon temporaire, si ces scripts sont nécessaires pour que le site s'affiche et fonctionne normalement.

### 6.1 Review Questions

- Comment peut-on effacer l'historique de navigation, les cookies et la mémoire cache du navigateur?
- Contre quels types d'attaques le module **NoScript** peut-il protéger votre système?

## Tor - anonymat et contournement sur Internet

### Short Description:

**Tor** est un logiciel conçu pour accroître le degré d'anonymat de vos activités sur Internet. Il camoufle votre identité et protège vos activités contre les technologies de surveillance sur Internet. **Tor** peut également être employé pour contourner le filtrage et les méthodes de censure de l'Internet.

### Online Installation Instructions:

#### Pour télécharger Tor

- Lisez la courte **Introduction aux Guides pratiques** <sup>[1]</sup>
- Cliquez sur l'icône **Tor** ci-dessous pour ouvrir la page <https://www.torproject.org/easy-download.html.fr>
- Défilez vers le bas, puis cliquez sur le lien **La version (en français) du Paquetage Tor pour Windows**
- **Sauvegardez** le fichier exécutable sur votre ordinateur, puis **double-cliquez** dessus pour lancer l'installation

- Après avoir complété l'installation de **Tor Browser**, vous pouvez supprimer l'exécutable d'installation.

Tor:



[214]

Site Internet

<https://www.torproject.org> [215]

Configuration requise

- Compatible avec toutes les versions de **Windows**
- Une connexion Internet
- Compatible avec tous les navigateurs populaires, en particulier **Mozilla Firefox**

Versions utilisées pour rédiger ce guide

- Tor Browser: 1.3.24

Licence

- Free/Libre Open Source Software

Lecture préalable

- Livret pratique Security in-a-box, chapitre **8. Préserver son anonymat et contourner la censure sur Internet** [216]

Niveau: 1: Débutant, 2: Moyen, 3: Intermédiaire, 4: Expérimenté, 5: Avancé

Temps d'apprentissage: 20 - 30 minutes

Ce que vous apportera l'utilisation de cet outil:

- La capacité de cacher votre identité numérique sur Internet.
- La capacité de déjouer vos **fournisseurs de service Internet** et les mécanismes de surveillance en dissimulant vos destinations en ligne.
- La capacité de contourner la censure et les règles de filtrage sur Internet.

Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows:

Il existe des versions du client de réseau de connexion anonyme **Tor** pour les systèmes d'exploitation \*GNU Linux\*\*, **Mac OS** et **Microsoft Windows**. **Tor** est l'outil en son genre le plus recommandé et le mieux testé. Nous vous présentons néanmoins d'autres solutions:

- **Hotspot Shield** [217] est une solution commerciale gratuite de **Réseau privé virtuel (VPN)** pour **Microsoft Windows**.
- **Dynaweb FreeGate** [218] est un outil de proxy gratuit pour **Microsoft Windows**.
- **UltraReach UltraSurf** [219] est un outil de proxy gratuit pour **Microsoft Windows**.
- **Your Freedom** [220] est un outil de proxy commercial qui offre également un service gratuit (quoique plus lent). Il est disponible en versions **Linux**, **Mac OS** et **Microsoft Windows**.
- **Psiphon** [221] est un proxy web et fonctionne donc avec tous les systèmes d'exploitation.

Nous suggérons fortement de lire la documentation conçue par **Sesawe** [222], une alliance mondiale vouée à la promotion de l'accès à l'information sans censure sur Internet.

## 1.1 À propos de cet outil

**Tor** est un logiciel conçu pour accroître le degré de sécurité et d'anonymat de vos activités et habitudes de navigation sur Internet. Il agit en camouflant votre identité et en brouillant la trace de vos activités sur Internet, afin que les technologies de surveillance soient incapables de vous retracer. Que l'anonymat soit important ou pas pour vous, **Tor** peut s'avérer un moyen utile et sécuritaire de promouvoir les libertés en ligne et contourner les mesures de censure sur Internet lorsque vous naviguez (ou publiez) sur certains sites ou carnets.

**Tor** protège votre anonymat en routant vos communications à travers un réseau décentralisé de serveurs/relais géré par des bénévoles un peu partout dans le monde. Cela empêche d'éventuels agents espions ou malveillants de surveiller votre connexion Internet pour savoir quels sites vous avez visités et/ou pour déterminer votre position géographique (où vous vous trouvez, sur quel ordinateur vous travaillez, etc.). Quant aux administrateurs bénévoles du réseau **Tor**, certains d'entre eux sont en mesure de savoir que vous utilisez le logiciel, et certains autres peuvent savoir que *quelqu'un* est en train d'accéder aux sites que vous visitez, mais personne ne peut détenir ces deux renseignements en même temps.

**Tor** peut camoufler vos tentatives de connexion à un site en particulier, mais n'a pas été conçu pour cacher le contenu de vos communications. En conséquence, **Tor** peut ajouter une couche supplémentaire de protection lorsque vous l'utilisez en combinaison avec d'autres services sécurisés comme **Riseup** ou **Gmail**, mais vous ne devriez pas utiliser ce programme pour accéder à des fournisseurs de service de courrier électronique non sécurisé, comme **Hotmail** ou **Yahoo**, ou tout autre site qui envoie ou reçoit des renseignements sensibles par une connexion *http* non sécurisée.

Définitions:

- **Port**: Dans ce guide, le terme « port » désigne un point d'entrée à travers lequel un logiciel peut communiquer avec des services se trouvant sur d'autres ordinateurs mis en réseau. Si une URL, comme **www.google.com**, vous fournit « l'adresse » d'un service, le port vous indique quelle « porte » utiliser lorsque vous arrivez à la bonne destination. Lorsque vous naviguez sur Internet, vous utilisez habituellement le port 80 pour les sites non sécurisés (**http://mail.google.com**) et le port 443 pour les sites sécurisés (**https://mail.google.com**).
- **Proxy**: Dans ce guide, le terme « proxy » désigne un logiciel intermédiaire – sur votre ordinateur, votre réseau local



ou quelque part d'autre sur Internet – qui contribue à relayer votre communication jusqu'à sa destination finale.

- **Route:** Dans ce guide, le terme « route » désigne le chemin de communication sur Internet entre votre ordinateur et le serveur de destination.
- **Relais passerelle:** Un relais passerelle (ou passerelle) est un serveur **Tor** qui facilite votre première entrée dans le réseau de connexion anonyme **Tor**. Les passerelles sont optionnelles et sont conçues pour être utilisées dans les pays où l'accès à **Tor** est bloqué.

#### Offline Installation Instructions :

#### Pour installer Tor

- \*Lisez la courte **Introduction** aux **Guides pratiques** <sup>[1]\*\*</sup>
- **Cliquez sur l'icône Tor ci-dessous** et 'Ouvrez' ou 'Exécutez' l'assistant d'installation. Si nécessaire, sauvegardez d'abord l'exécutable sur votre ordinateur, puis double-cliquez sur l'icône pour lancer l'assistant.
- Lisez attentivement les 'Consignes d'installation' dans la prochaine section avant de poursuivre l'installation.
- Si vous avez sauvegardé l'exécutable sur votre ordinateur, vous pouvez le supprimer après l'installation.

Tor:





[223]

## Comment extraire le paquetage du navigateur Tor

### 2.0 Comment extraire le paquetage du navigateur Tor

Le **paquetage du navigateur Tor** contient tout ce dont vous avez besoin pour naviguer en sécurité sur Internet: le programme **Tor**, **Polipo**, **Vidalia**, la version portable de **Firefox** et le module complémentaire **Torbutton** pour **Firefox**. Ce paquetage ne requiert aucune installation; vous n'avez qu'à l'extraire et l'exécuter.

Pour extraire le **paquetage du navigateur Tor**, suivez les étapes énumérées ci-dessous:

**Première étape.** Double-cliquez sur  tor-browser-1.3.24\_fr ; il est possible que la boîte de dialogue *Fichier ouvert - Avertissement de sécurité* s'affiche. Le cas échéant, cliquez sur  pour afficher la fenêtre suivante:

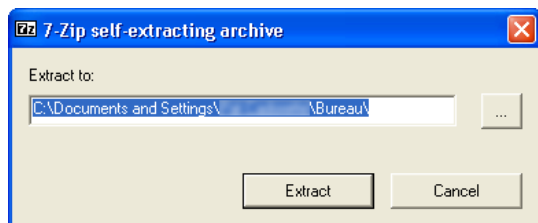


Figure 1: La fenêtre 7-Zip self-extracting archive

**Note:** Le **paquetage du navigateur Tor** ne s'installe pas automatiquement dans le répertoire *C:\Program Files*, contrairement aux procédures d'installation de la majorité des outils que nous recommandons.

**Important:** Il est également possible d'installer et d'utiliser le **paquetage du navigateur Tor** sur une clé USB. Cela peut vous permettre de dissimuler le fait que vous utilisez **Tor** sur votre ordinateur.

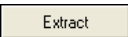


**Deuxième étape.** Cliquez, soit sur  pour accepter le répertoire par défaut, soit sur  pour afficher la fenêtre *Rechercher un dossier*:



Figure 2: La fenêtre Rechercher un dossier

**Troisième étape.** Naviguez jusqu'au dossier désiré pour installer le **paquetage du navigateur Tor**, puis cliquez sur  pour confirmer votre choix, tel qu'illustré ci-dessous:

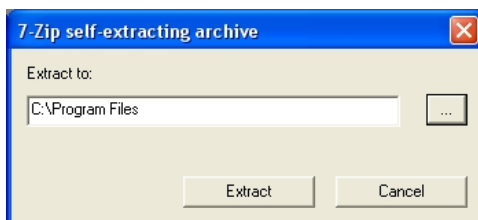


Figure 3: Un exemple de chemin d'installation pour le paquetage du navigateur Tor

**Quatrième étape.** Cliquez sur  pour lancer l'extraction des fichiers et dossiers du **paquetage du navigateur Tor** et afficher la fenêtre de progression suivante:

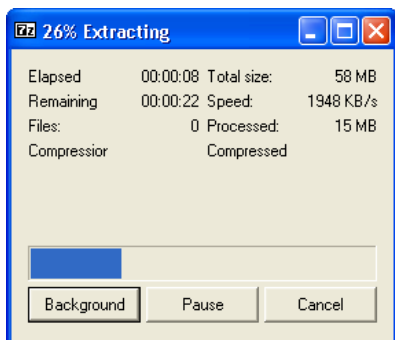


Figure 4: La fenêtre de progression de l'extraction

Dans le présent exemple, à l'issue du processus d'extraction, le **paquetage du navigateur Tor** apparaît dans le chemin de répertoire *C: Program Files\Tor Browser*, tel qu'illustré ci-dessous:

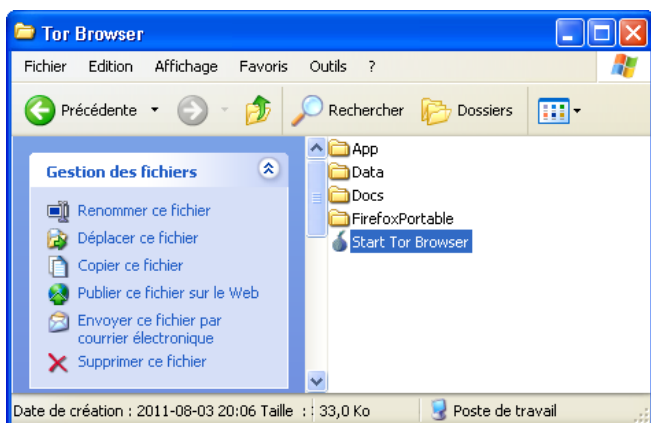


Figure 5: Le paquetage du navigateur Tor installé dans le répertoire Program Files

Vous avez complété l'extraction du **paquetage du navigateur Tor**.

Veillez maintenant poursuivre la lecture du guide [Comment accéder à Internet par l'intermédiaire du réseau Tor](#) <sup>[224]</sup> pour commencer à naviguer sur Internet de façon anonyme et sécurisée.

## Comment accéder à Internet par l'intermédiaire du réseau Tor

Sommaire des sections de cette page:

- [3.0 À propos de l'accès au réseau Tor](#)
- [3.1 Comment se connecter au réseau Tor](#)
- [3.2 Comment vérifier manuellement votre connexion au réseau Tor](#)
- [3.3 Comment naviguer sur Internet en utilisant Tor](#)
- [3.3.1 Comment configurer Mozilla Firefox pour fonctionner avec Tor](#)
- [3.3.2 Comment configurer Internet Explorer pour fonctionner avec Tor](#)

---

### 3.0 À propos de l'accès au réseau Tor


Pour commencer à naviguer anonymement sur Internet, vous devez lancer le programme **Navigateur Tor**. Dans un premier temps, le programme connectera votre système au réseau **Tor**. Une fois que la connexion au réseau **Tor** sera établie, le **Navigateur Tor** lancera automatiquement une instance distincte du **Firefox portable** qui est inclus dans le **Paquetage du navigateur Tor**.

**Note:** Il y a un compromis nécessaire entre l'anonymat et la vitesse d'exécution. Puisque **Tor** facilite la navigation anonyme, son utilisation ralentira considérablement la navigation. **Tor** fait transiter votre navigation par les ordinateurs de

nombreux bénévoles situés un peu partout dans le monde afin de protéger votre sécurité et votre identité.

### 3.1 Comment se connecter au réseau Tor

Pour se connecter au réseau **Tor**, suivez les étapes énumérées ci-dessous:

**Première étape.** Naviguez jusqu'au dossier du *Navigateur Tor*, puis **double-cliquez** sur  pour afficher la fenêtre suivante:

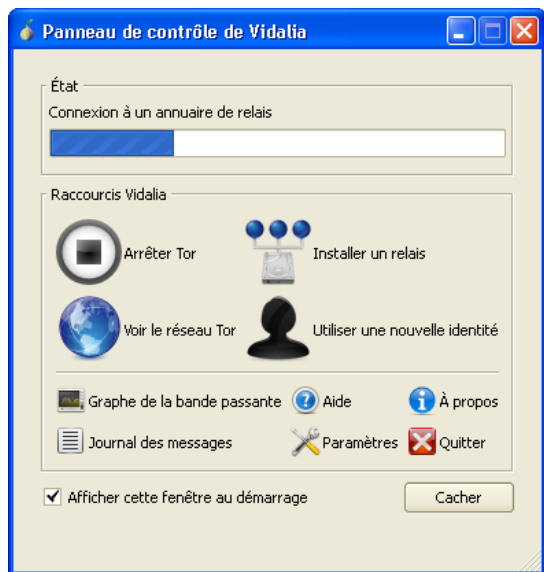




Figure 1: Le panneau de contrôle de Vidalia en cours de connexion au réseau Tor

Lorsque le *Panneau de contrôle de Vidalia* établit une connexion au réseau **Tor**, un icône ressemblant à un oignon jaune apparaît dans la *barre des tâches*, comme suit: . Une fois que la connexion a été établie entre votre ordinateur et le réseau **Tor**, l'icône devient vert: .

**Note:** Pour apprendre à utiliser efficacement le *Panneau de contrôle de Vidalia*, veuillez consulter la page **Comment utiliser le Panneau de contrôle de Vidalia** <sup>[225]</sup>.

Quelques secondes plus tard, le *Navigateur Tor* activera le navigateur **Mozilla Firefox** affichant la fenêtre suivante:

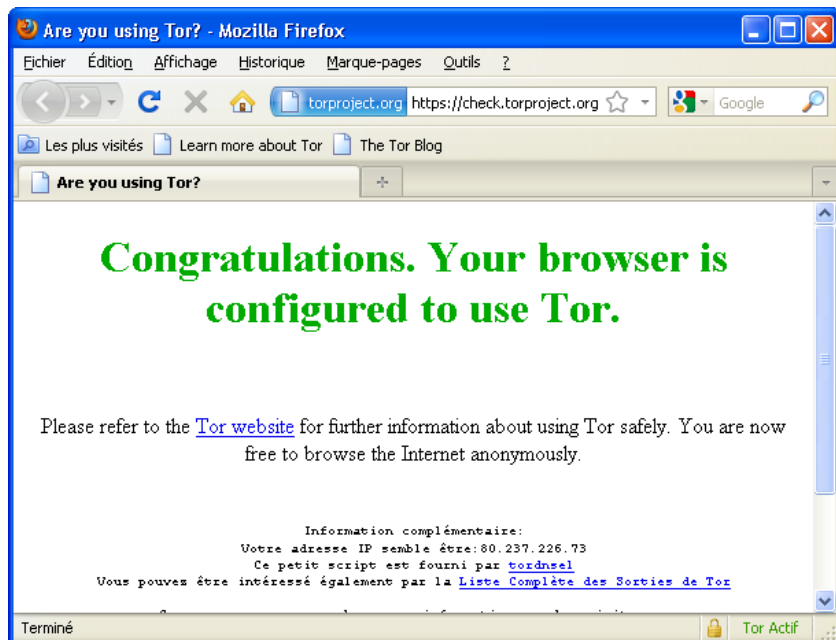




Figure 2: Mozilla Firefox affichant l'onglet Are you using Tor?

Chaque fois que vous lancez le programme **Navigateur Tor**, ce dernier active automatiquement le *Panneau de contrôle Vidalia* (Figure 1) et la fenêtre <https://check.torproject.org/> <sup>[226]</sup> (Figure 2). Le module complémentaire **Torbutton** apparaît également dans le coin inférieur droit de la fenêtre, comme suit: .

**Note:** Par contre, si une fenêtre de navigation de **Mozilla Firefox** était déjà ouverte lorsque vous avez lancé le **Navigateur Tor**, le **Torbutton** apparaîtra en mode désactivé dans cette même fenêtre, comme suit: .

Le **Torbutton** est utilisé pour configurer **Firefox** afin de se connecter adéquatement au réseau **Tor**. Vous n'avez qu'à cliquer sur le **Torbutton** pour alterner entre les modes actif et inactif.

Cependant, si vous n'êtes pas connecté au réseau **Tor**, le **Torbutton** sera désactivé et la fenêtre suivante s'affichera:

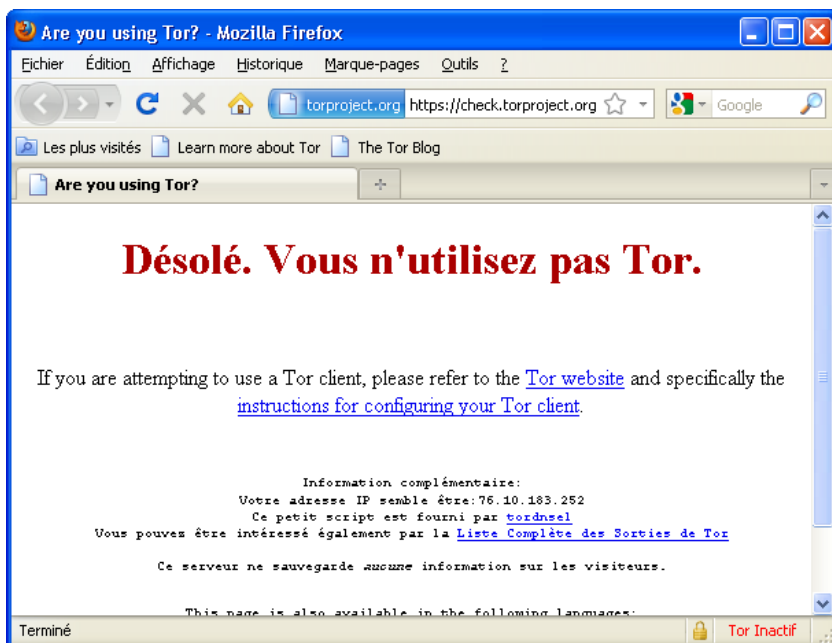


Figure 3: Mozilla Firefox affichant l'onglet Désolé, vous n'utilisez pas Tor

Si la Figure 3 s'affiche, si le **Torbutton** est désactivé (malgré vos tentatives pour l'activer) ou si la page de navigation est vide, veuillez consulter la section [5.0 Résolution des problèmes courants sous Tor](#) [227].

## 3.2 Comment vérifier manuellement votre connexion au réseau Tor

Pour vérifier manuellement si vous êtes connecté ou non au réseau **Tor**, suivez les étapes énumérées ci-dessous:

**Première étape.** Ouvrez le site Internet <https://check.torproject.org/> [226]. Ce site confirmera si vous êtes connecté ou non au réseau **tor**.

Si votre navigateur Internet est connecté à l'Internet par l'entremise du réseau **Tor**, les sites qui sont bloqués ou restreints dans votre pays seront désormais accessibles, et vos activités en ligne seront privées et sécurisées. Vous remarquerez peut-être également que certaines pages Web, tel que [www.google.com](http://www.google.com), se comporteront occasionnellement comme si vous vous trouviez dans un autre pays. Cela est normal lorsqu'on utilise **Tor**.

## 3.3 Comment naviguer sur Internet en utilisant Tor

Bien qu'il vous soit possible de commencer immédiatement à naviguer sur Internet avec **Firefox** par l'entremise du réseau **Tor**, nous vous recommandons de lire la section suivante pour régler **Firefox** de sorte que votre sécurité et votre anonymat en ligne soient optimisées.

### 3.3.1 Comment modifier les paramètres de Mozilla Firefox pour Tor

Le **torbutton** est un module complémentaire pour **Mozilla Firefox**. Il s'agit d'un petit programme conçu pour protéger l'anonymat et la sécurité de vos activités en ligne en bloquant certaines vulnérabilités de **Mozilla Firefox**.

**Important:** Des sites malveillants, ou même un serveur **Tor**, pourraient *quand-même* révéler des renseignements sur votre emplacement et vos activités en ligne, et ce, *même* lorsque vous utilisez **Tor**. Heureusement, la configuration par défaut de **Torbutton** est relativement sécuritaire; cependant, nous vous recommandons de modifier certains paramètres pour optimiser votre sécurité et la protection de votre vie privée.

**Note:** Les utilisateurs **avancés** qui ont une compréhension approfondie des enjeux de sécurité associés aux navigateurs voudront peut-être raffiner encore davantage leurs paramètres.

La fenêtre des *Préférences Torbutton* comporte trois onglets qui vous permettent de régler diverses options:

- L'onglet **Paramètres du proxy**
- L'onglet **Paramètres de sécurité**
- L'onglet **Paramètres d'affichage**

Il est facile d'accéder à la fenêtre des *Préférences Torbutton*, que **Torbutton** soit activé ou non. Pour afficher la fenêtre des *Préférences Torbutton*, suivez les étapes énumérées ci-dessous:

**Première étape.** Cliquez à droite sur le **Torbutton** pour afficher son menu, comme suit:

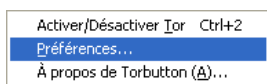


Figure 4: Le menu de Torbutton

**Deuxième étape.** Sélectionnez l'item *Préférences...* pour afficher la fenêtre suivante:

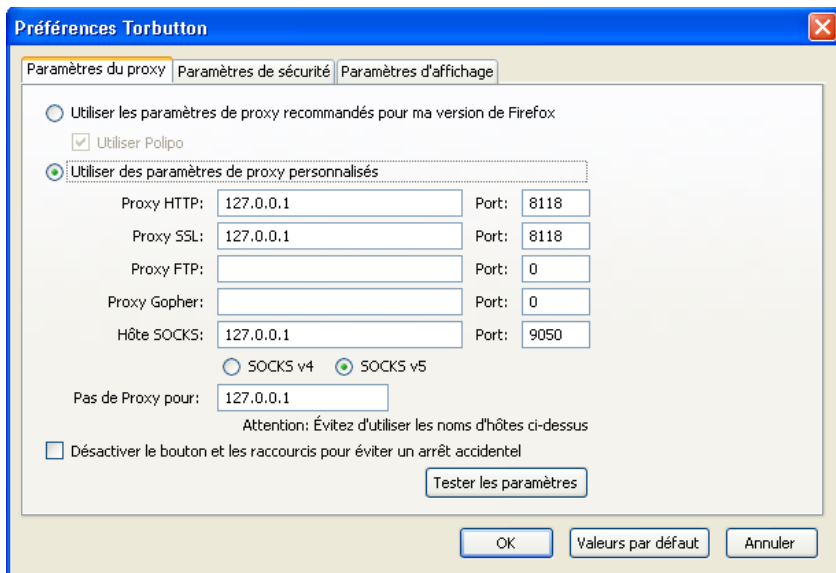


Figure 5: La fenêtre des préférences de Torbutton affichant l'onglet Paramètres du proxy

- L'onglet **Paramètres du proxy**

L'onglet *Paramètres du proxy* permet de déterminer comment **Firefox** accède à l'Internet quand le **Torbutton** est activé. Vous ne devriez pas avoir à changer quoi que ce soit dans cet onglet.

- L'onglet **Paramètres de sécurité**

L'onglet *Paramètres de sécurité* est conçu pour les utilisateurs *expérimentés* et *avancés* qui ont une compréhension approfondie des navigateurs et de la sécurité sur Internet. Ses paramètres par défaut présentent un niveau élevé de sécurité pour les utilisateurs moyens. Ces *Paramètres de sécurité* vous permettent de déterminer comment **Torbutton** gère l'historique de navigation, la mémoire cache, les cookies et d'autres fonctions de **firefox**.

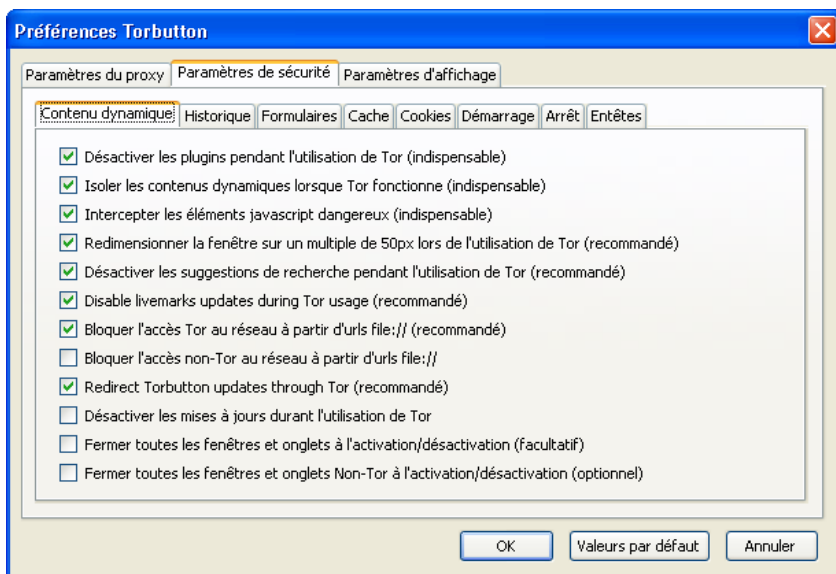




Figure 6: L'onglet Paramètres de sécurité

L'option *Désactiver les plugins pendant l'utilisation de Tor (indispensable)* est l'un des quelques paramètres de sécurité que vous pourriez devoir activer, quoique *temporairement*. Pour afficher des contenus vidéo en ligne avec **Tor**, y compris avec les services de **DailyMotion** [228], **The Hub** [229] et **YouTube** [230], vous devez **décocher** l'option *Désactiver les plugins pendant l'utilisation de Tor*.

**Note:** Vous ne devriez activer que les plugins des sites de confiance, et vous devez retourner à l'onglet *Paramètres de sécurité* et **re-cocher** l'option *Désactiver les plugins pendant l'utilisation de Tor* lorsque vous aurez complété votre visite de ces sites.

Pour plus d'information sur les fonctions particulières de chaque option de l'onglet **Paramètres de sécurité**, veuillez consulter la page **Torbutton** [231].

- L'onglet **Paramètres d'affichage**

L'onglet *Paramètres d'affichage* vous permet de déterminer comment s'affiche le **Torbutton** dans la barre d'état de **Firefox**, soit **Tor Actif** ou , ou **Tor Inactif** ou . La fonctionnalité opère de façon identique d'une manière ou d'une autre.

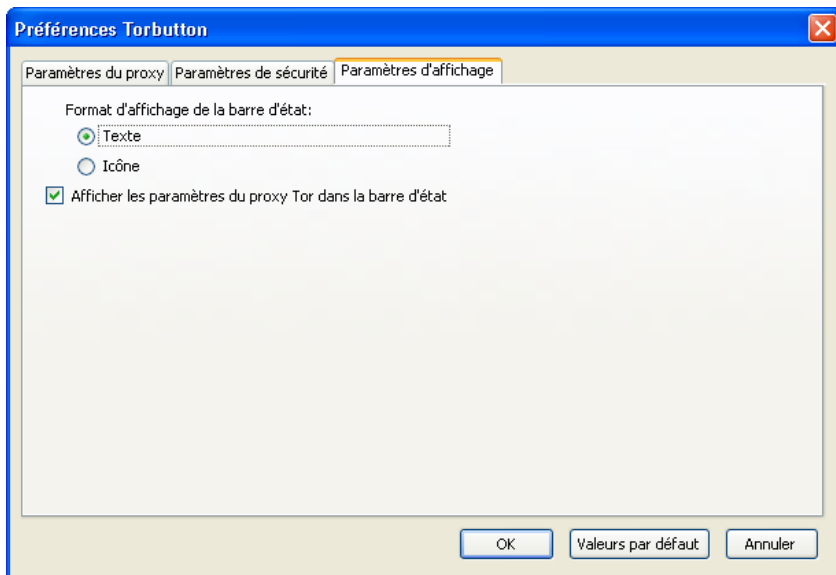


Figure 7: L'onglet Paramètres d'affichage

**Conseil:** Lorsque vous avez terminé votre consultation, assurez-vous de supprimer votre cache de fichiers temporaires et vos cookies. Cela peut être fait dans **Firefox** en **sélectionnant Outils > Supprimer l'historique récent...**, **cochant** toutes les options disponibles dans la fenêtre qui s'affiche, puis en **cliquant** sur le bouton *Effacer maintenant*. Pour plus d'information à ce sujet, veuillez consulter le chapitre du **Guide pratique** portant sur **[Mozilla Firefox]** ([fr/firefox\\_privacy\\_and\\_security](http://fr/firefox_privacy_and_security)).

Pour plus d'information sur le **Torbutton**, veuillez consulter la page **Torbutton FAQ** <sup>[232]</sup>.

### 3.3.2 Comment configurer Internet Explorer pour fonctionner avec Tor

**Note:** Bien que **Tor** soit conçu pour fonctionner avec n'importe quel navigateur, **Firefox** et **Tor** constituent une combinaison idéale pour éviter d'être détecté par des parties malveillantes ou hostiles. Idéalement, **Internet Explorer** ne devrait être utilisé qu'en dernier ressort!

Cela dit, si vous êtes dans une situation où l'utilisation d'**Internet Explorer** est complètement inévitable, suivez les étapes énumérées ci-dessous:

**Première étape.** Ouvrez le navigateur **Internet Explorer**.

**Deuxième étape.** Sélectionnez **Outils > Options Internet** pour afficher la fenêtre *Options Internet*.

**Troisième étape.** Cliquez sur l'onglet *Connexions* pour afficher la fenêtre illustrée à la *Figure 8* ci-dessous:

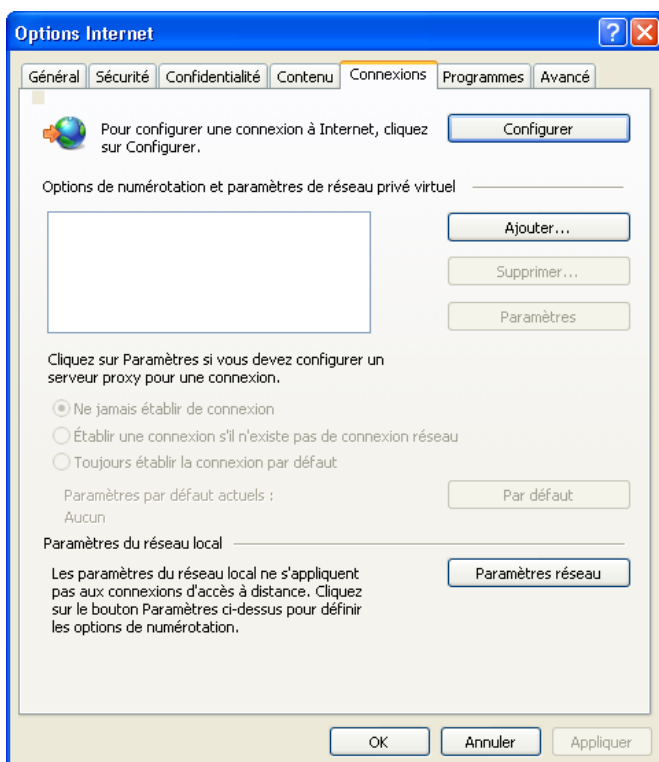


Figure 8: L'onglet Connexions de la fenêtre Options Internet

**Quatrième étape.** Cliquez sur **Paramètres réseau** pour afficher la fenêtre *Paramètres du réseau local* illustrée ci-dessous:

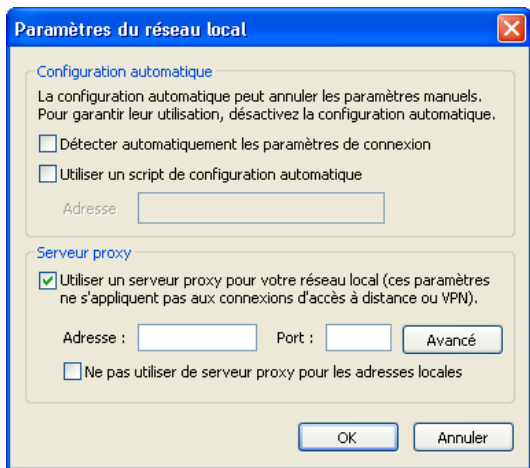


Figure 9: La fenêtre des Paramètres du réseau local

**Cinquième étape.** Cochez l'option *Utiliser un serveur proxy...*, tel qu'illustré à la figure 9 ci-dessus, puis cliquez sur **Avancé** pour afficher la fenêtre des *Paramètres du proxy*.

**Sixième étape.** Remplissez les zones des paramètres du proxy tel qu'illustré ci-dessous:

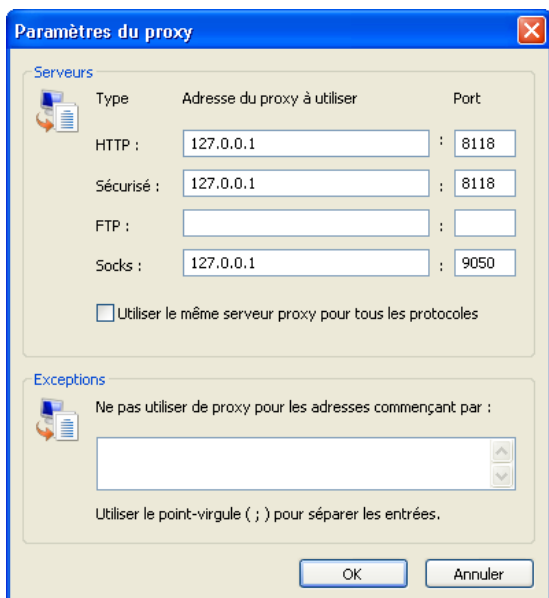


Figure 10: Un exemple de fenêtre de paramètres du proxy

**Septième étape.** Cliquez sur **OK** sur chacune des fenêtres de configuration ci-dessus pour sortir de la fenêtre **Options Internet** et revenir au navigateur **Internet Explorer**.

**Note:** Vous devrez répéter les **étapes 1 à 4** pour cesser d'utiliser **Tor**. Au lieu de l'**étape 5**, vous devriez **désactiver** l'option *Utiliser un serveur proxy...*

**Conseil:** Vous devez vider le cache des fichiers Internet temporaires et supprimer les cookies et l'historique de navigation à la fin de votre séance de navigation en suivant les étapes énumérées ci-dessous:

**Première étape.** Sélectionnez **Outils > Options Internet** pour afficher l'onglet *Général* par défaut, tel qu'illustré ci-dessous:

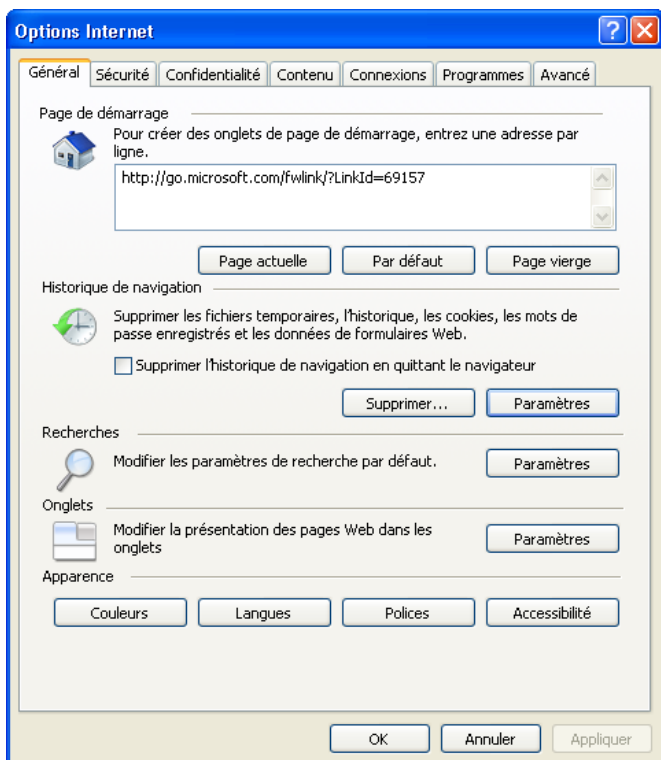


Figure 11: L'onglet Général des Options Internet d'Internet Explorer

Deuxième étape. Cliquez sur  dans la section *Historique de navigation* pour afficher la fenêtre *Supprimer l'historique de navigation*:

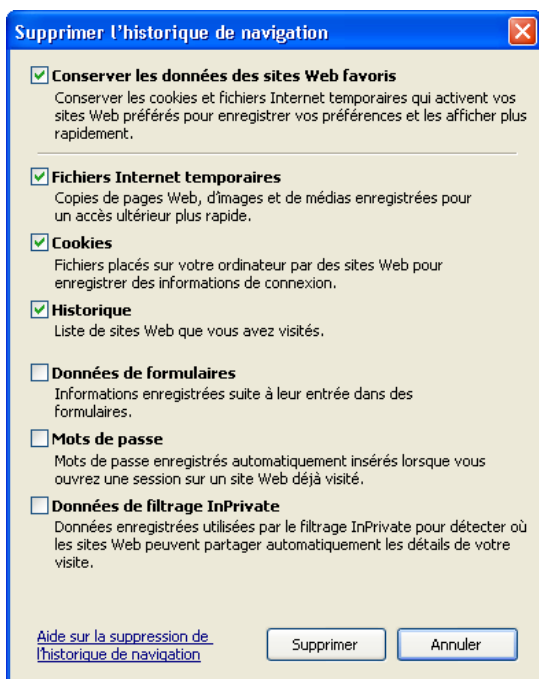


Figure 12: la fenêtre *Supprimer l'historique de navigation*

Troisième étape. Cochez *Fichiers Internet temporaires*, *Cookies* et *Historique*.

Quatrième étape. Cliquez sur  pour supprimer les Fichiers Internet temporaires, les Cookies et l'Historique de navigation.

**Note:** Pour accéder au réseau Tor avec Internet Explorer, vous devez laisser fonctionner le **Navigateur Tor** avec **Vidalia** connecté au réseau Tor.

## Comment utiliser le panneau de contrôle de Vidalia

- [4.0 À propos du Panneau de contrôle de Vidalia](#)
- [4.1 Pour visualiser la connexion au réseau Tor](#)
- [4.2 Pour visualiser et régler les paramètres du Panneau de contrôle de Vidalia](#)
- [4.3 Pour interrompre et relancer le service Tor](#)



## 4.0 À propos du Panneau de contrôle de Vidalia

Le *Panneau de contrôle de Vidalia*, avec lequel vous êtes désormais familier, est le principal interface graphique du programme **Tor**. Le *Panneau de contrôle de Vidalia* vous permet de régler les paramètres principaux de **Tor** et de visualiser les paramètres de connexion.

Pour ouvrir le *Panneau de contrôle de Vidalia*, suivez les étapes énumérées ci-dessous:

**Si le Navigateur Tor est déjà en fonction, double-cliquez** sur  pour lancer le *Panneau de contrôle de Vidalia*.

**Conseil:** Si vous cliquez à droite sur l'icône représentant un oignon vert, le *Panneau de contrôle de Vidalia* s'affichera sous forme de menu contextuel, tel qu'illustré ci-dessous:

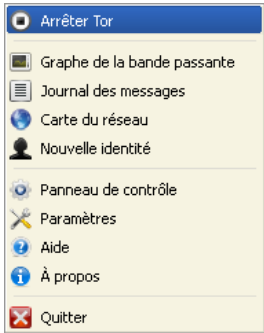



Figure 1: Le menu contextuel du Panneau de contrôle de Vidalia

**Si le Navigateur Tor n'est pas déjà en fonction, naviguez** jusqu'au dossier du **Navigateur Tor**, puis **double-cliquez** sur  Start Tor Browser.exe pour activer le *Panneau de contrôle de Vidalia* et vous connecter automatiquement au réseau **Tor**, comme suit:

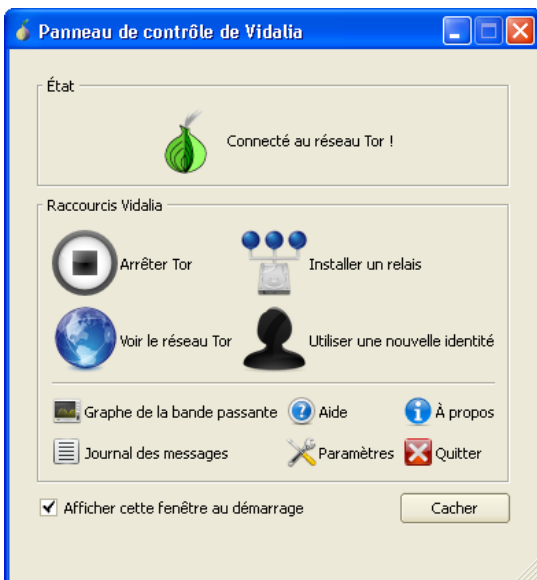


Figure 2: Le Panneau de contrôle de Vidalia affichant le message Connecté au réseau Tor

## 4.1 Pour visualiser la connexion au réseau Tor

Première étape. Cliquez sur  pour afficher la fenêtre suivante:

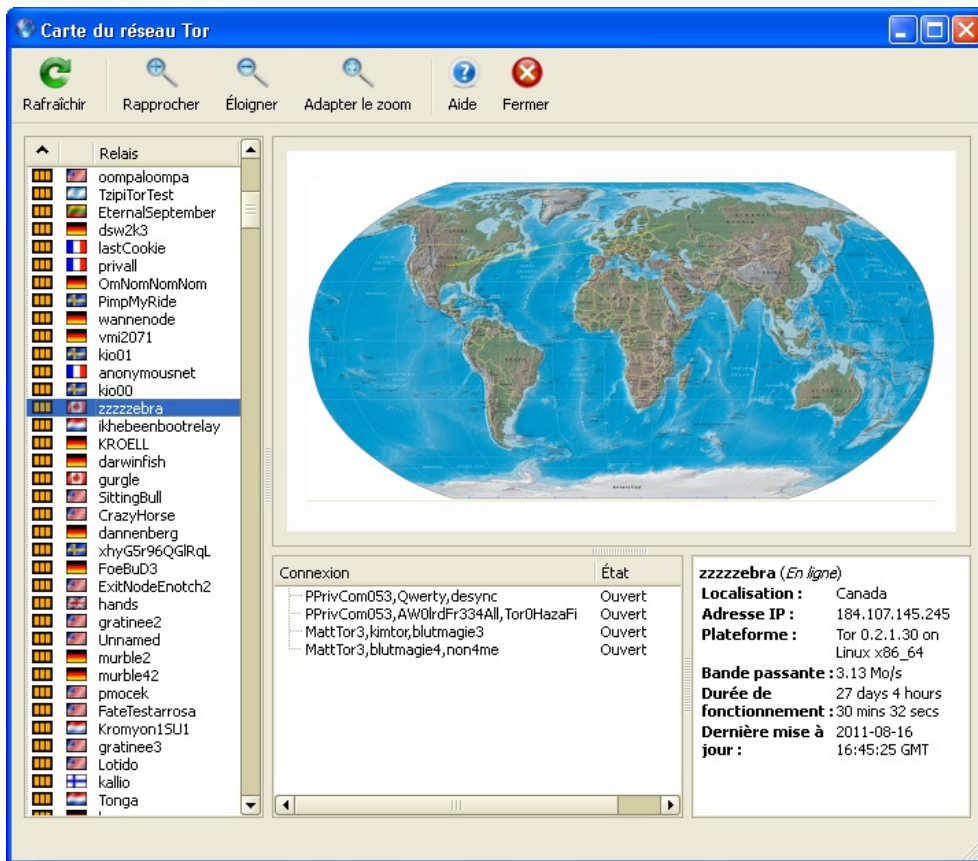



Figure 3: La carte du réseau Tor

La *Carte du réseau Tor* liste tous les relais **Tor** disponibles qui composent actuellement le réseau de connexion anonyme **Tor**. Le panneau de gauche liste ces serveurs en fonction de leur bande passante disponible et de leur situation géographique.

- Cliquez sur  pour lister ces serveurs en ordre ascendant ou descendant de la bande passante disponible, ou en ordre alphabétique du pays d'origine.


Sous la mappemonde se trouvent deux panneaux, le panneau *Connexion* et le panneau où s'affichent les détails du relais. Le panneau *Connexion* affiche les noms des serveurs **Tor** choisis au hasard comme relais de votre connexion anonyme.

- Choisissez un serveur dans la liste *Connexion* pour visualiser le trajet emprunté par votre connexion dans le réseau **Tor**, illustré par des lignes vertes sur la carte.

Le panneau adjacent affiche les détails de connexion des serveurs relais listés dans le panneau *Relais* à gauche; à la *Figure 3*, les détails de connexion d'un serveur relais situé au Canada, *zzzzzebra*, sont affichées.

**Note:** La *Carte du réseau Tor* sert à illustrer comment **Tor** fonctionne en présentant des idées abstraites et des renseignements complexes sur un mode graphique.

## 4.2 Pour visualiser et régler les paramètres du Panneau de contrôle de Vidalia

Première étape. Cliquez sur  Paramètres pour afficher la fenêtre suivante:

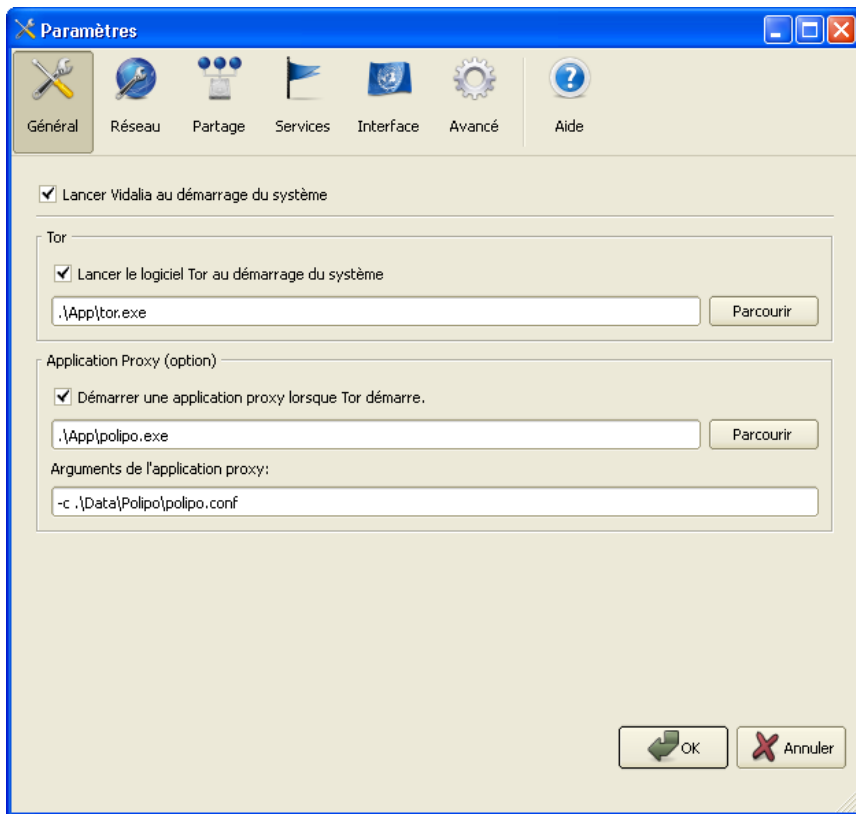


Figure 4: La fenêtre des paramètres du Panneau de contrôle de Vidalia

L'onglet *Général* vous permet d'indiquer si **Vidalia** doit être lancé automatiquement à chaque démarrage de **Windows** et si **Tor** devrait être également lancé à ce moment.

Si vous préférez lancer le programme **Vidalia** manuellement, vous n'avez qu'à **décocher** l'option *Lancer Vidalia au démarrage du système*.

**Note:** Nous recommandons aux utilisateurs **débutants** ou **moyens** d'accepter les paramètres par défaut, tel qu'illustré à la Figure 4.

**Deuxième étape.** Cliquez sur  pour enregistrer vos paramètres.

Bien que la langue par défaut du programme **Tor** soit l'anglais, l'onglet *Interface* vous permet une autre langue d'interface pour le *Panneau de contrôle de Vidalia*. Cet onglet vous permet en outre de modifier l'apparence du programme.

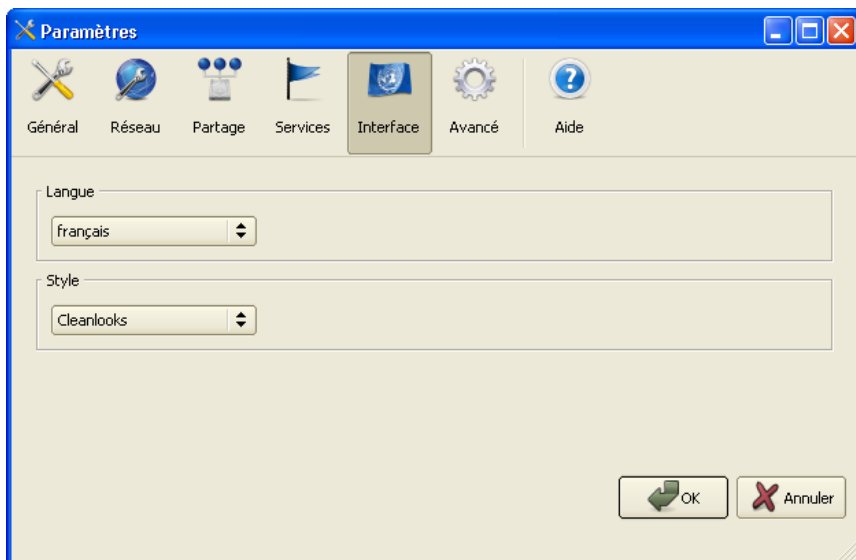


Figure 5: L'onglet Interface des paramètres du Panneau de contrôle de Vidalia

### 4.3 Pour interrompre et relancer le service Tor

**Première étape.** Cliquez sur  dans le panneau *Raccourcis Vidalia* pour interrompre le programme **Tor**;

la section *État* du *Panneau de contrôle de Vidalia* s'affiche alors comme suit:

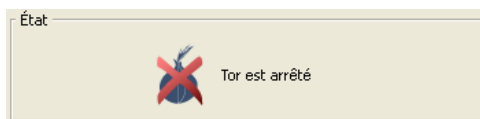


Figure 6: La section de l'état de Tor affichant le message Tor est arrêté



Deuxième étape. Cliquez sur **Lancer Tor** pour relancer le programme **Tor**; après quelques secondes, la section *État* du *Panneau de contrôle de Vidalia* s'affiche alors comme suit:

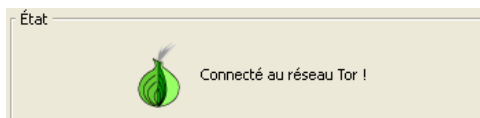


Figure 7: La section de l'état de Tor affichant le message Connecté au réseau Tor!

## Résolution des problèmes courants sous Tor

- [5.0 À propos de la résolution des problèmes courants sous Tor](#)
- [5.1 Comment afficher le Journal des messages](#)
- [5.2 Comment régler les paramètres réseau de Tor](#)


### 5.0 À propos de la résolution des problèmes courants sous Tor

Plusieurs facteurs peuvent faire en sorte que **Tor** ne fonctionne pas normalement. Certains des problèmes les plus courants sont décrits ci-dessous, avec des suggestions de solutions appropriées. Toutes les fonctions décrites dans cette section sont accessibles par le *Panneau de contrôle de Vidalia*.

**Note:** Plusieurs erreurs courantes peuvent être réglées tout simplement en redémarrant votre système ou en répétant l'extraction du **Paquetage du navigateur Tor**.

### 5.1 Comment afficher le Journal des messages

Vous pouvez consulter le journal des messages de **Tor** même lorsque le programme tente d'établir une connexion initiale au réseau **Tor**. Cela peut vous aider à déterminer si le logiciel fonctionne et, si ce n'est pas le cas, de trouver les causes du ou des problèmes.

Première étape. Cliquez sur  **Journal des messages** pour afficher la fenêtre *Journal des messages*, puis cliquez sur l'onglet *Advanced* pour afficher cette fenêtre:

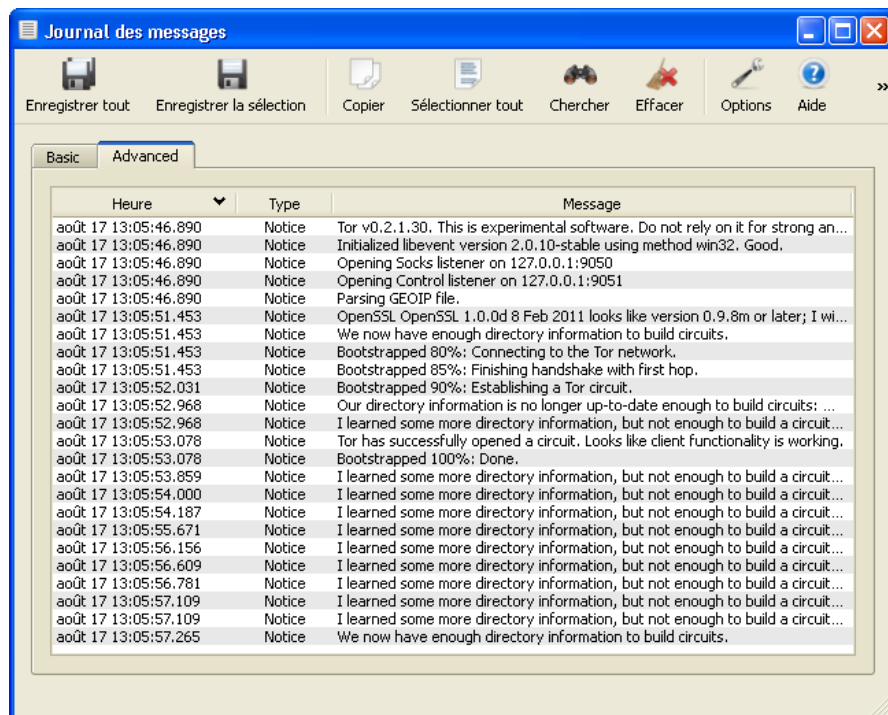


Figure 1: Le Journal des messages de Vidalia

Le journal montre que **Tor** a été lancé et continuera à afficher des messages portant sur le fonctionnement de **Tor**. Ne vous inquiétez pas trop du signalement concernant le "experimental software". Malgré ce qui est indiqué ici, **Tor** est l'outil de connexion anonyme le mieux éprouvé à ce jour.


## 5.1.1 Pour comprendre les messages d'erreurs les plus courants

Il existe cependant quelques messages d'erreur importants que vous devriez chercher si vous éprouvez des difficultés avec le programme **Tor**; en voici la description:

- *connection\_create\_listener(): Could not bind to 127.0.0.1:9050: Address already in use. Is Tor already running?*

Ce message signifie qu'un autre processus **Tor** a déjà été entamé. La solution la plus simple dans ce cas est de fermer tous les programmes de **Vidalia** et de redémarrer votre ordinateur.

- *Vidalia was unable to start Tor. Check your settings to ensure the correct name and location of your Tor executable is specified*

Cette erreur se produit lorsque **Vidalia** est incapable de trouver le fichier exécutable de **Tor**, *tor.exe*, qui devrait normalement ressembler à ceci: . Pour résoudre ce problème, suivez les étapes énumérées ci-dessous:

**Première étape.** Redémarrez votre ordinateur et essayez de lancer le **Navigateur Tor** à nouveau. Si l'erreur persiste, exécutez la *Deuxième étape*, ci-dessous:

**Deuxième étape.** Supprimez le dossier actuel du **Navigateur Tor**, puis téléchargez la plus récente version du **Paquetage du Navigateur Tor**. Procédez à l'extraction du **Paquetage du Navigateur Tor**, puis Lancez le programme.

- *I have learned some directory information, but not enough to build a circuit*

Ce message peut apparaître de façon répétée lorsque **Tor** démarre, et peut même continuer à s'afficher par la suite si vous avez une connexion Internet particulièrement lente. Ce message signifie simplement que **Tor** continue à télécharger de l'information à propos du réseau afin d'établir un circuit **Tor** ou une connexion à votre système.

Lorsque **Tor** est enfin prêt à être utilisé, le journal affiche le message suivant :

- *Tor has successfully opened a circuit. Looks like client functionality is working.*

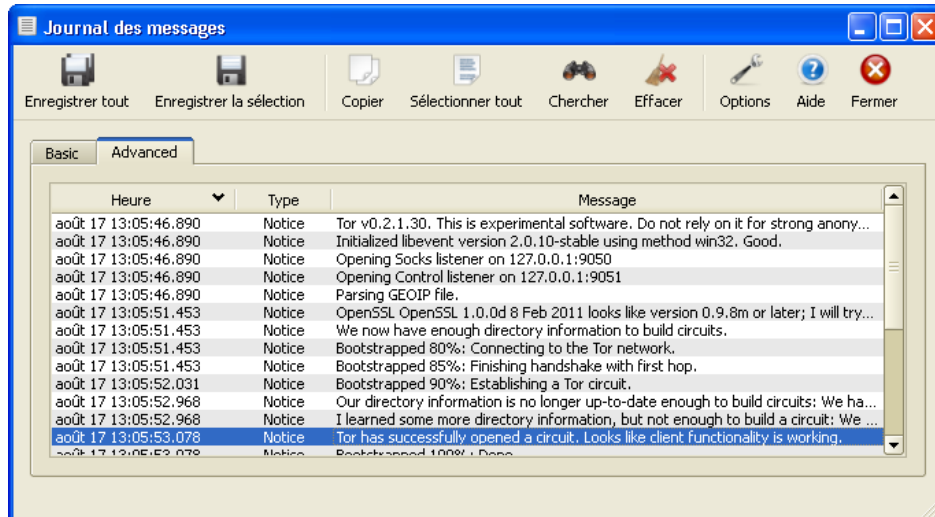


Figure 2: Un message confirmant la connexion (surligné en bleu)

Ce message indique que **Tor** a réussi à établir une route à travers son réseau et semble fonctionner normalement.

**Note:** Même si vous utilisez **Mozilla Firefox**, vous devez encore activer le **Torbutton** avant de pouvoir naviguer sur Internet de façon anonyme. Si vous utilisez un autre navigateur, vous devez d'abord régler les paramètres du proxy pour être en mesure de vous connecter à Internet via **Tor**.

Si le journal n'affiche aucun nouveau message pendant quinze minutes après avoir affiché le message *Opening Control listener* ou le message *Tor has learned some directory information, but not enough to build a circuit*, il vous faudra peut-être ajuster les paramètres réseau de **Tor**. Il est possible que votre connexion Internet actuelle exige que vous utilisiez un proxy Web particulier, ou bloque certains ports. Il est par ailleurs possible que votre gouvernement ou votre fournisseur de service Internet ait bloqué l'accès au réseau **Tor**.

## 5.2 Comment régler les paramètres réseau de Tor

Si vous vous rendez compte que **Tor** ne fonctionne plus normalement ou que le programme n'arrive pas à se connecter lorsque vous l'installez et le lancez, il vous faudra peut-être modifier les paramètres réseau du programme. Les paramètres de connexion au réseau se rapportent au serveur proxy, au ports et aux relais passerelles, comme nous le verrons dans cette section.

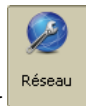
Vous devez peut-être suivre ces quelques étapes.

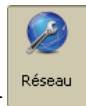


**Première étape.** Cliquez sur **Arrêter Tor** dans le **Panneau de contrôle de Vidalia** pour interrompre le service **Tor**.



**Deuxième étape.** Cliquez sur **Paramètres** pour afficher la fenêtre **Paramètres**.



Troisième étape. Cliquez sur  pour afficher le contenu de l'onglet Réseau, comme suit:

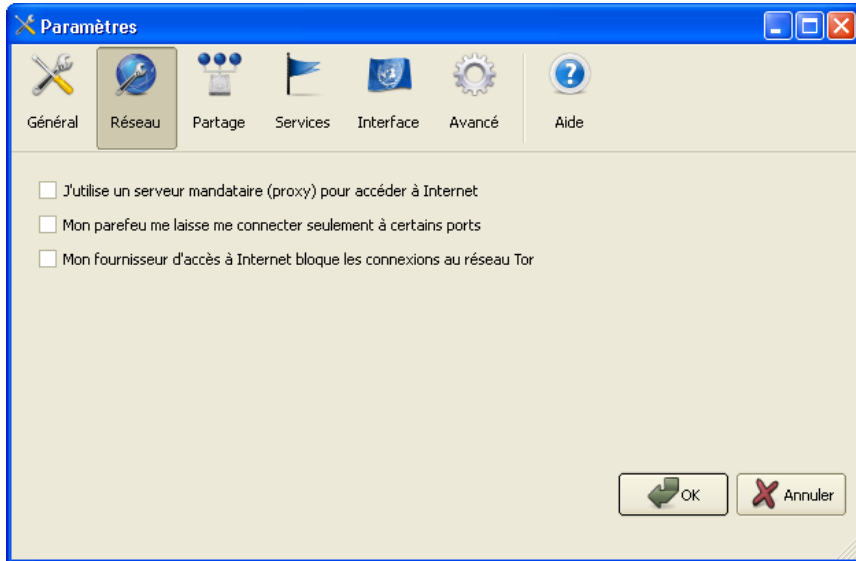
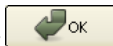



Figure 3: L'onglet Réseau de la fenêtre Paramètres

Quatrième étape. Cliquez sur  pour accepter les paramètres, fermer la fenêtre Paramètres, puis cliquez sur  dans le Panneau de contrôle de Vidalia pour lancer Tor.

### 5.2.1 Utiliser un serveur mandataire (proxy)

Si vous devez utiliser un serveur mandataire (ou proxy) pour accéder à Internet, saisissez les renseignements nécessaires dans cette fenêtre. En règle générale, cela est plutôt requis par les réseaux de sociétés privées ou universitaires, mais des serveurs proxys sont occasionnellement requis par des cafés Internet, ou même par le gouvernement pour couvrir l'accès à Internet dans certains pays. Si les renseignements de proxy nécessaires ne sont pas clairement indiqués, vous devrez peut-être vous adresser à un administrateur du réseau ou à une personne qui utilise la même connexion Internet que vous.

Première étape. Cochez l'option *J'utilise un serveur mandataire (proxy) pour accéder à Internet*.

Deuxième étape. Saisissez les renseignements du proxy dans les zones appropriées:

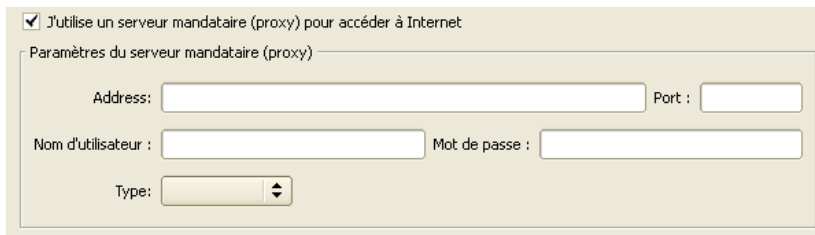


Figure 4: La section Paramètres du proxy

### 5.2.2 Gérer les restrictions de ports

Certains réseaux ou paramètres informatiques peuvent restreindre l'accès à certains ports. Si vous êtes en mesure de naviguer normalement sur Internet, vous pouvez compter sur au moins deux ports ouverts (80 et 443). Vous pouvez régler Tor pour fonctionner exclusivement avec ces deux ports.

Première étape. Cochez l'option *Mon parefeu me laisse me connecter seulement à certains ports*.

Deuxième étape. La zone *Ports autorisés* devrait afficher '80,443', tel qu'illustré à la Figure 5 ci-dessous:

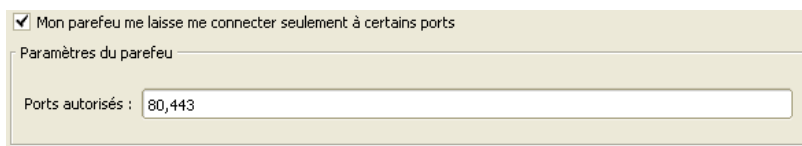


Figure 5: La section Paramètres du pare-feu affichant les ports ouverts sur le réseau

### 5.2.3 Utiliser un relais passerelle

Si vous ne pouvez toujours pas vous connecter au réseau Tor, il vous reste encore deux options:

**Première option:** Consultez le wiki [Tor FAQ wiki](#) <sup>[233]</sup> pour trouver des suggestions de marches à suivre.

**Deuxième option:** Vous résidez peut-être dans l'un des quelques pays qui bloquent activement l'accès à **Tor**. Dans ce cas, vous devrez utiliser un *relais passerelle* pour établir une connexion avec le réseau **Tor**.

Les *passerelles Tor* vous permettent d'accéder au réseau anonyme **Tor**, même si l'accès en est bloqué de l'intérieur de votre pays, en intégrant une 'première étape' cachée dans le réseau. Pour utiliser cette fonction, vous devez indiquer l'emplacement d'au moins une passerelle. Idéalement, vous devriez saisir l'adresse de trois passerelles ou plus. Si vous connaissez une personne de confiance qui utilise déjà une passerelle, vous pouvez lui demander de partager ces renseignements avec vous.

Vous pouvez aussi utiliser une des deux méthodes proposées par la *Base de données de passerelles* du **Projet Tor**.


**Méthode 1:** Envoyez un courriel à [[bridges\[at\]torproject\[dot\]org](#)], à partir de n'importe quel compte **Gmail**, avec les mots "get bridges" dans le corps du message. La base de données vous acheminera alors les adresses de trois passerelles. (N'oubliez pas, vous devriez TOUJOURS vous connecter à votre compte **Gmail** par la page <https://mail.google.com> <sup>[234]</sup>!).

**Méthode 2:** Fermez le programme **Tor** et rendez-vous au site Internet de la *Base de données de passerelles* du **Projet Tor** à <https://bridges.torproject.org/> <sup>[235]</sup> (sans utiliser **Tor**), qui affiche les renseignements associés à trois passerelles différentes.

**Note:** La *Base de données de passerelles* est conçue pour empêcher qui que ce soit de se renseigner facilement sur toutes les adresses de passerelles, c'est pourquoi il est possible que les mêmes passerelles s'affichent chaque fois que vous effectuez une requête en vous connectant au site. Si vous attendez suffisamment longtemps, de nouvelles adresses s'afficheront.

**Première étape.** Cochez l'option *Mon fournisseur d'accès à Internet bloque les connexions au réseau Tor*.

**Deuxième étape.** Coupez et collez ou saisissez l'adresse d'un relais passerelle dans la zone *Ajouter une passerelle*, tel qu'illustré à la *Figure 6*. Les renseignements de la passerelle comprennent une adresse IP et un numéro de port, comme 79.47.201.97:443, et peuvent aussi inclure une longue série de chiffres et de lettres à la fin, comme par exemple 80E03BA048BFFEB4144A4359F5DF7593A8BBD47B.

**Troisième étape.** Cliquez sur  pour ajouter l'adresse dans le panneau qui se trouve sous la zone de texte *Ajouter une passerelle*.

**Quatrième étape.** Répétez les étapes 2 et 3 pour chaque nouvelle adresse de passerelle. Il est recommandé d'en saisir au moins trois. Pour en saisir davantage, vous devrez peut-être attendre que la base de données de passerelles s'actualise.



Figure 6: Ajouter une adresse de relais passerelle

## Faq et questions récapitulatives

### 6.0 Faq et questions récapitulatives


**Tor** est un logiciel extrêmement bien testé et entretenu. Le réseau de connexion anonyme **Tor** est utilisé par des milliers de personnes, un peu partout sur la planète, et des améliorations constantes en ont fait un système de plus en plus stable et sûr. Même si certaines des explications apportées dans ce guide peuvent sembler complexes, dans la plupart des cas, vous n'aurez même pas à dépasser la section **3.0 Comment accéder à Internet par l'intermédiaire du réseau Tor** <sup>[236]</sup> pour être en mesure d'utiliser le programme normalement.

Mansour a lu attentivement le **chapitre 8** <sup>[237]</sup> du livret pratique, qui porte sur les mesures de contournement de la censure, et il vient tout juste de terminer la lecture du Guide pratique **Tor**. Il lui reste cependant quelques questions pour Magda qui, elle, utilise **Tor** depuis plusieurs années.

**Q:** Pourquoi devrais-je utiliser **Tor**?

**R:** Bonne question. **Tor** est un outil fort pratique pour contourner la censure sur Internet afin d'accéder à certains sites. Ce programme est aussi très utile si l'on souhaite cacher les sites que l'on visite à notre fournisseur de service Internet, ou encore si l'on ne veut pas que les sites Internet puissent déterminer où l'on se trouve.

**Q:** Il y a un message d'erreur dans le Journal des messages que je ne comprends pas. Que devrais-je faire?

R: Consulte le wiki **Tor FAQ** <sup>[238]</sup> wiki pour voir si ton message s'y trouve. Sinon, tu peux également cliquer sur  À propos dans le **Panneau de contrôle de Vidalia** et jeter un coup d'oeil au chapitre **Résolution des problèmes courants sous Tor** <sup>[227]</sup>.

Q: Lorsque je lance le **Navigateur Tor**, est-ce que tous mes autres programmes communiquent de façon anonyme via le **Réseau Tor**?

R: Non, il est très important de se rappeler qu'il faut se connecter au **Réseau Tor** uniquement avec le navigateur **Firefox** muni du module complémentaire **Torbutton**. Tous les autres programmes communiquent directement avec les autres serveurs sur Internet. Pour être absolument certain de communiquer via le **Réseau Tor**, tu peux toujours vérifier manuellement la connexion sur le site <https://check.torproject.org>. Par ailleurs, **Tor** s'appuie sur l'exercice de la prudence, du bon sens et du jugement de la part des utilisateurs lorsque ceux-ci visitent des sites inconnus ou peu familiers.

Q: Est-ce que **Tor** protège toutes les communications faites à partir de mon navigateur **Firefox**?

R: **Tor** chiffre toutes les communication entre ton ordinateur et le réseau **Tor**. Cependant, il faut tenir compte du fait que **Tor** ne peut pas chiffrer le trafic entre le réseau **Tor** et le site Internet avec lequel tu communique. Pour ce faire, **tu dois utiliser le protocole HTTPS** ou d'autres modes de chiffrement similaires, d'autant plus si tu attaches beaucoup d'importance à la sécurité et au caractère privé de tes renseignements!

## 6.1 Questions récapitulatives

- Combien de serveurs **Tor** sont utilisés pour établir une connexion via le réseau **Tor**?
- Où peut-on trouver davantage d'information à propos de ces serveurs?
- Quels paramètres doivent être modifiés dans votre navigateur Internet pour que celui-ci puisse accéder à des pages Internet via **Tor**?
- Quels sont les programmes qui doivent être activés pour que vous soyez en mesure d'accéder au réseau **Tor**?
- Comment peut-on faire en sorte que l'interface Vidalia ne soit pas lancée chaque fois que **Windows** démarre?

## Outils de réseautage social: Facebook, Twitter et autres

### Short Description:

Ce chapitre a pour but de vous aider à naviguer à travers les paramètres de confidentialité et de sécurité de certains sites populaires de réseautage social et d'en rendre leur utilisation *plus sûre*, ou disons plutôt, *moins hasardeuse*. En particulier, il donne des conseils étape par étape sur **Facebook** et **Twitter**, tout comme des indications générales sur l'utilisation de **YouTube** et **Flickr**.

Ces sites de réseaux sociaux sont les outils de réseautage social les plus populaires et les plus utilisés. Ils appartiennent à des entreprises privées et, comme il est indiqué dans le chapitre **10. Savoir se protéger sur les sites de réseautage social** <sup>[239]</sup>, ces entreprises gagnent de l'argent en collectant des informations sur les utilisateurs et en les revendant à des annonceurs. Une répression gouvernementale prendra en premier ces sites pour cible et les bloquera; les entreprises céderont aux pressions gouvernementales et procéderont à des censures si nécessaire. D'autres sites peuvent offrir une alternative intéressante, tels que **Diaspora** <sup>[240]</sup>, **Crabgrass** <sup>[241]</sup>, **Friendica** <sup>[242]</sup>, **Pidder** <sup>[243]</sup> ou **SecureShare** <sup>[244]</sup> qui ont été conçus pour un usage activiste en toute sécurité. **Social Swarm** <sup>[245]</sup> est un think-tank dirigé par un organisme sans but lucratif, qui mène des discussions, des activités de sensibilisation et des campagnes liées à la confidentialité sur les réseaux sociaux; et il peut être une ressource d'apprentissage utile.

Des sites similaires sont peut-être plus populaires dans d'autres régions et il se peut que vous souhaitiez explorer d'autres options. Avant de faire votre choix, tenez compte des points suivants :

1. Fournit-il une connexion via **SSL** pour toutes les utilisations du site plutôt que seulement durant la connexion ? Y-a-t-il des problèmes concernant le chiffrement tels que des problèmes liés à des certificats de chiffrement ?
2. Lisez attentivement le Contrat de Licence Utilisateur Final et la politique de confidentialité ou d'utilisation des données. Comment sont traités vos contenus et données ? Avec qui sont-ils partagés ?
3. Quelles options de confidentialité sont fournies aux utilisateurs ? Pouvez-vous choisir de partager vos vidéos en toute sécurité avec un petit nombre d'individus, ou bien sont-elles toutes publiques par défaut ?
4. Connaissez-vous l'**emplacement géographique des serveurs**, la juridiction territoriale dont ils relèvent ou l'endroit où l'entreprise est inscrite ? Savez-vous en quoi cette information concerne la confidentialité et la sécurité de l'usage de votre adresse électronique et de vos informations ? Les propriétaires du site vont-ils transmettre des informations s'ils reçoivent une demande gouvernementale l'exigeant ?

## Guide de sécurisation de Facebook

**Facebook** est un site populaire de réseautage social dont l'accessibilité est quasi universelle. Il est donc extrêmement important de connaître et de contrôler ses paramètres de confidentialité.

### Page d'accueil

- [www.facebook.com](http://www.facebook.com) <sup>[246]</sup>

### Configuration de l'ordinateur

- Une connexion Internet
- **Navigateur web Firefox avec des extensions de sécurité** <sup>[247]</sup> OU **Navigateur web Tor** <sup>[248]</sup>

### Lecture obligatoire

- Livret pratique, chapitre **10. Savoir se protéger sur les sites de réseautage social** <sup>[249]</sup>
- **Conditions d'utilisation** <sup>[250]</sup> et **Politique d'utilisation des données** <sup>[251]</sup> de **Facebook**



Temps nécessaire pour commencer à utiliser cet outil : 40 minutes

Ce que vous obtenez en retour :

- L'aptitude à **réduire** la quantité d'informations personnelles rendues publiques lorsque vous utilisez **Facebook**.
- L'aptitude à **contrôler** qui peut accéder à votre profil, vos mises à jour, photos et autres données sur **Facebook**, et quand ils peuvent y accéder.
- L'aptitude à **réduire** la quantité d'informations personnelles rendues disponibles à un tiers, y compris les partenaires publicitaires et sites web associés à **Facebook**.

## 1.1 Ce qu'il faut savoir sur cet outil avant de commencer

**Facebook** est le site de réseautage social le plus populaire au monde. Il peut être et a été largement utilisé par les défenseurs des droits de l'homme dans le but de constituer des réseaux, de communiquer, d'organiser et promouvoir des événements ou des débats. Cependant, il s'agit également d'une source d'information potentiellement riche pour ceux qui s'opposent aux activités des défenseurs de droits. Il est donc extrêmement important de connaître les différents paramètres de compte et de confidentialité.

**Facebook** est contrôlé par le gouvernement des États-Unis et est fort probablement surveillé par d'autres gouvernements. En outre, la politique d'utilisation des données de **Facebook** déclare que vos informations seront communiquées en cas de demandes légales, y compris dans le cadre d'enquêtes gouvernementales.

Il est important de garder à l'esprit qu'en raison de la nature ouverte de **Facebook**, votre sécurité et votre vie privée dépendent fortement de celles de vos amis et contacts. Le fait de mettre ces conseils seul en pratique aidera à préserver votre vie privée et votre sécurité, vos efforts auront toutefois moins d'efficacité si vos contacts **Facebook** ne les pratiquent pas également. Il est donc important de diffuser ces techniques auprès de vos amis, votre famille et autres contacts sur **Facebook** dans le but d'améliorer votre sécurité tout comme la leur.

Il vous faut toujours être à jour quant aux **paramètres de confidentialité de Facebook**. Les paramètres décrits dans le présent guide vous aideront à garder votre compte **Facebook** sécurisé (mise à jour mai 2012). Toutefois, il est conseillé de consulter la page d'aide officielle de Facebook pour toutes les mises à jour concernant les paramètres de confidentialité et de sécurité - ou pour toute question que vous puissiez avoir : <https://www.facebook.com/help/privacy>.

Plus plus d'informations sur la **Politique d'utilisation des données** <sup>[252]</sup> de **Facebook**, consultez ces infographiques sur le site **Me and My Shadow** <sup>[253]</sup>.

# Comment modifier les paramètres généraux du compte Facebook

Liste des sections de cette page:

- [2.0 Comment créer un compte Facebook](#)
- [2.1 Conseils pour les paramètres généraux du compte](#)
- [2.2 Paramètres de sécurité sur Facebook](#)
- [2.3 Abonnés](#)
- [2.4 Paramètres des applications](#)

---

## 2.0 Comment créer un compte Facebook

Pour créer un compte **Facebook**, ouvrez votre navigateur web, (nous recommandons le **navigateur web Firefox avec des extensions de sécurité** <sup>[247]</sup> ou le **navigateur Tor** <sup>[248]</sup>), et tapez <https://www.facebook.com> dans la barre d'adresse pour accéder à la page d'accueil de **Facebook**. Notez que le **s** dans l'adresse [https](https://www.facebook.com) indique que vous communiquez via une connexion sûre, chiffrée (aussi connue sous le nom de *Secure Socket Layer* - *SSL*).

**Étape 2.** Remplissez les champs intitulés **Prénom**, **Nom de famille**, **Votre adresse électronique** et **Mot de passe**.

## Inscription

C'est gratuit (et ça le restera toujours)

Prénom :

Nom de famille :

Votre adresse électronique :

Saisissez à nouveau votre adresse électronique :

Nouveau mot de passe :

Je suis :

Anniversaire :

Pourquoi dois-je indiquer ma date de naissance ?

En cliquant sur Inscription, vous acceptez nos Conditions et reconnaissez avoir lu et comprendre notre Politique d'utilisation des données, y compris Utilisation des cookies.

Graphique 2 : Un formulaire rempli

**Note :** Sachez que si vous utilisez votre vrai nom et votre adresse électronique courante pour créer votre compte **Facebook**, les autorités ou des adversaires vous trouveront plus facilement. Il est donc plus sûr de créer une nouvelle adresse électronique et d'utiliser un surnom, que vous pourrez ensuite communiquer à vos amis et contacts. Pour plus d'informations sur la préservation de l'anonymat en ligne, voir le chapitre **8. Préserver votre anonymat et contourner la censure sur Internet** [237].

**Note :** Rappelez-vous qu'il est extrêmement important de choisir un mot de passe fort pour protéger votre compte et vos informations. Consultez s'il vous plaît le chapitre **3. Créer et sauvegarder des mots de passe sûrs** [54].

**Étape 3.** Assurez-vous d'avoir lu et compris les **conditions d'utilisation** [250] et la **politique d'utilisation des données** [251] de **Facebook** avant de cliquer sur *Inscription*. Elles contiennent des informations importantes sur les renseignements que vous confiez à **Facebook** et la façon dont ils seront utilisés par eux. Pour plus d'informations sur la politique d'utilisation des données de **Facebook**, consultez ces infographies sur le site **Me and My Shadow** [253].

**Étape 4.** Sur l'écran *Retrouver vos amis*, **Facebook** vous demande de fournir votre adresse électronique et votre mot de passe afin de chercher dans votre compte e-mail des contacts abonnés à **Facebook** que vous pourrez ajouter plus tard à vos contacts **Facebook**. Nous vous recommandons d'**ignorer cette étape**.

Étape 1  
Retrouvez vos amis

Étape 2  
Informations du profil

Étape 3  
Photo du profil

### Vos amis sont-ils déjà sur Facebook ?

Un certain nombre de vos amis peuvent déjà s'y trouver. La recherche dans votre compte de messagerie est la façon la plus rapide de retrouver vos amis sur Facebook. [Découvrez comment faire.](#)

 **Google Mail**

Votre adresse :

[Retrouver des amis](#)

 **Windows Live Hotmail** [Retrouver des amis](#)

 **Web.de** [Retrouver des amis](#)

 **Autre service de courrier électronique** [Retrouver des amis](#)

[Ignorer cette étape](#)

Graphique 3 : L'écran Retrouver vos amis

**Étape 5.** Sur l'écran *Informations du profil*, **Facebook** vous demande de fournir des informations sur le collègue/lycée ou l'université que vous avez fréquentés et sur votre employeur actuel. Cette information peut certes aider vos amis à vous retrouver, mais facilitera également la tâche à vos adversaires. Demandez-vous bien s'il est vraiment nécessaire pour vous de fournir cette information. Il est peut-être plus conseillé de **donner de fausses informations** et de vous rendre introuvable pour toute personne qui vous cherche. Vous pouvez également **ignorer cette étape** si vous ne souhaitez pas fournir ces informations.

À partir des informations que vous fournissez à cette étape, **Facebook** va vous suggérer d'anciens camarades de classe ou de probables collègues que vous souhaitez peut-être ajouter à vos contacts. Encore une fois, réfléchissez bien à qui

vous souhaitez ajouter à vos contacts et **n'ajoutez aucune personne à vos contacts que vous ne connaissez pas ou en qui vous n'avez pas confiance.**

Si vous ne souhaitez pas ajouter des amis à ce stade, vous pouvez également **ignorer cette étape.**

Étape 1  
Retrouvez vos amis

Étape 2  
Informations du profil

Étape 3  
Photo du profil

### Remplissez votre profil

Cette information vous aidera à retrouver vos amis sur Facebook.

Collège/lycée :   ▼

Université :   ▼

Employeur :   ▼

← Préc. Ignorer - **Enregistrer et continuer**

Graphique 4 : L'écran Informations du profil

**Étape 6.** Sur l'écran *Photo du profil*, **Facebook** vous demande de fournir une photo de vous-même, soit en **téléchargeant** une, soit en **prenant** une photo avec votre webcam.

Étape 1  
Retrouvez vos amis

Étape 2  
Informations du profil

Étape 3  
Photo du profil

### Choisissez l'image de votre profil



**télécharger une photo**  
À partir de votre ordinateur

- ou -

**Prendre une photo**  
Avec votre webcam

← Préc. Ignorer - **Enregistrer et continuer**

Graphique 5 : L'écran Photo du profil

**Note :** Cette image, tout comme votre image de couverture pour votre timeline **Facebook**, sera visible à quiconque accédant à votre profil, **y compris à des personnes qui ne sont pas vos amis** et indépendamment de vos paramètres de confidentialité. Demandez-vous bien si vous souhaitez utiliser une photo dans laquelle vous, vos amis, collègues, votre famille ou organisation peuvent être reconnus par de possibles adversaires.

Une fois que vous avez cliqué sur *Ignorer* ou *Enregistrer et continuer*, vous serez invité à vérifier la boîte de réception de l'adresse électronique que vous avez fournie. Vous y trouverez un e-mail de **Facebook** vous demandant de cliquer sur un lien pour confirmer la validité de votre adresse électronique. Une fois ce geste accompli, votre page **Facebook** est créée.

## 2.1 Conseils pour les paramètres généraux du compte

**Étape 7.** Sur votre page d'accueil **Facebook**, **cliquez** sur la petite flèche en haut à droite à côté de *Accueil* et sélectionnez *Paramètres du compte*.

□

Graphique 6 : Le menu Paramètres

Ceci vous mène au menu *Paramètres du compte*. Le premier onglet s'intitule *Paramètres généraux du compte*. Vous pouvez y modifier les informations concernant votre nom, nom d'utilisateur, adresse électronique, mot de passe, réseaux et langue.

The screenshot shows the Facebook account settings page for 'Tom Testeur'. The page is titled 'Paramètres généraux du compte'. On the left, there is a navigation menu with options: Général, Sécurité, Notifications, Espace Assistance, Abonnés, Applications, Mobile, Paiements, Publicités Facebook, and Cadeaux. The main content area displays the following settings:

Nom	Tom Testeur	Modifier
Nom d'utilisateur	http://www.facebook.com/tom.testeur.71	Modifier
Adresse électronique	Principale : tom.testeur@gmail.com	Modifier
Mot de passe	Mot de passe jamais changé.	Modifier
Réseaux	Aucun réseau.	Modifier
Langue	Français (France)	Modifier

Below the table, there is a link: 'Télécharger une copie de vos données sur Facebook.'

At the bottom left, there is a note: 'Vous pouvez également accéder à vos paramètres de confidentialité ou modifier votre journal pour contrôler qui voit ces informations.'

Graphique 7 : Paramètres généraux du compte

**Étape 8.** Demandez-vous bien si vous souhaitez utiliser vos vrais nom et adresse électronique pour créer votre compte **Facebook**. Des autorités ou adversaires pourront vous trouver plus facilement. Il serait donc plus sûr d'utiliser une autre adresse électronique et un pseudonyme que vous pourrez ensuite communiquer à vos amis et contacts. Votre nom et votre adresse électronique peuvent être facilement modifiés en cliquant dessus dans ce menu, ce qui ouvre un second menu déroulant. Pour plus d'informations sur la préservation de votre anonymat en ligne, voir le chapitre **8. Préserver votre anonymat et contourner la censure sur Internet** [237].

The screenshot shows the 'Nom' settings form. It includes the following fields and options:

- Prénom : Tom
- Deuxième prénom : Facultatif
- Nom de famille : Testeur
- Afficher en tant que : Tom Testeur
- Autre nom : Facultatif [?]
- Inclure sur mon profil
- Mot de passe : [Empty field]

Buttons: Enregistrer les modifications, Annuler

Graphique 8 : Options pour le nom

**Step 9.** Vous devez mettre votre mot de passe régulièrement **à jour**, de préférence au moins une fois tous les trois mois. Rappelez-vous qu'il est extrêmement important de choisir un mot de passe fort pour protéger votre compte et vos informations. Consultez s'il vous plaît le chapitre **3. Créer et sauvegarder des mots de passe sûrs du guide pratique** [54].

The screenshot shows the 'Mot de passe' settings form. It includes the following fields and options:


- Actuel : [Masked password]
- Nouveau : [Masked password]
- Saisir à nouveau : [Masked password]
- Mots de passe identiques

Buttons: Enregistrer les modifications, Annuler

Graphique 9 : Options pour le mot de passe

**Étape 10.** Votre réseau. **Facebook** vous permet de rejoindre des réseaux basés sur des critères tels que votre lycée, université, employeur, ville natale ou ville actuelle afin que l'on vous trouve et que l'on se connecte à vous plus facilement. Ceci peut certes vous aider à trouver des contacts plus facilement, mais facilitera également la tâche à des adversaires vous cherchant. Étant donné le nombre d'utilisateurs de ce site, il est improbable que vous ayez besoin de joindre un réseau pour vous connecter sur **Facebook** avec des gens que vous connaissez et en qui vous avez confiance.

## 2.2 Paramètres de sécurité Facebook

**Étape 11.** Cliquez sur  Sécurité à gauche dans le menu. Ceci ouvre la page des paramètres de sécurité.

## Security Settings

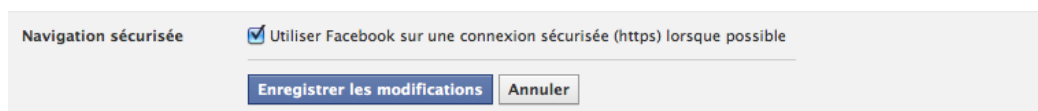
Secure Browsing	Secure browsing is currently enabled.	<a href="#">Edit</a>
Login Notifications	Login notifications are disabled.	<a href="#">Edit</a>
Login Approvals	Approval is <b>not</b> required when logging in from an unrecognized device.	<a href="#">Edit</a>
App Passwords	You haven't created app passwords.	<a href="#">Edit</a>
Recognized Devices	No recognized devices.	<a href="#">Edit</a>
Active Sessions	Logged in from Berlin, BE, DE and 6 other locations.	<a href="#">Edit</a>

[Deactivate your account.](#)

Graphique 10 : Page des paramètres de sécurité

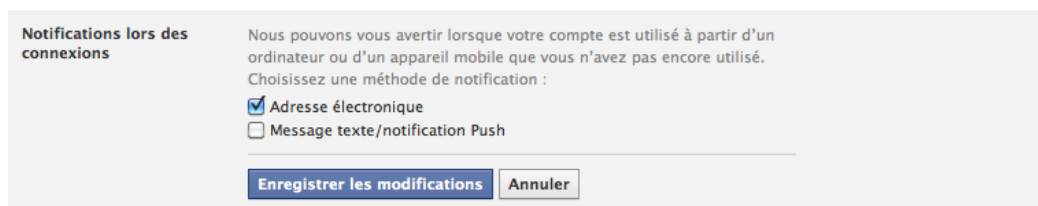
**Étape 12.** Cliquez sur l'onglet **Navigation sécurisée** et, dans le menu qui s'affiche, cochez la case *Utiliser Facebook sur une connexion sécurisée (https) lorsque possible*, et cliquez sur **Enregistrer les modifications**. Ceci assurera que votre ordinateur communique avec le site via une connexion **Secure Socket Layer (SSL)** par défaut.

**Note :** Même activée, la SSL ne s'applique pas à Facebook Chat. Si vous voulez discuter avec un contact à propos d'un sujet sensible, il est recommandé de **ne pas** utiliser Facebook Chat dans ce but. Pour savoir comment bien chatter, consultez le chapitre **7. Préserver la confidentialité de vos communications sur Internet du guide pratique** [126].



Graphique 11 : Options Navigation sécurisée

**Étape 13.** **\*\*Cliquez** sur l'onglet *Notifications lors des connexions*. Ici, vous pouvez choisir d'être averti si quelqu'un tente de se connecter à votre page **Facebook** à partir d'un dispositif que vous n'avez pas encore utilisé. Choisissez une méthode de notification par e-mail ou par Message texte / notification Push.



Graphique 12 : Options Notifications lors des connexions

**Étape 14.** Pour plus de sécurité, vous pouvez choisir d'entrer un code de sécurité à chaque fois que l'on accède à votre compte à partir d'un ordinateur ou d'un dispositif que **Facebook** ne reconnaît pas. Le code de sécurité vous sera envoyé par SMS sur votre téléphone portable.

**Note** Ceci signifie que vous devrez fournir votre numéro de portable à **Facebook**, ce qui permet de prouver que vous êtes le propriétaire de ce compte **Facebook**. L'avantage de cette option est qu'elle permet une vérification supplémentaire lors de la connexion; ce qui peut faciliter la connexion à votre compte en utilisant des outils de contournement (tels que **Tor Browser** [248], proxy, VPN, etc).

Si vous décidez d'activer cette option, **cliquez** sur l'onglet *Approbatons de connexion* et suivez les instructions données pour sa mise en place.



Graphique 13 : Options Approbatons de connexion

**Étape 15.** Cliquez sur l'onglet *Sessions actives*, visible dans le *Graphique 10* ci-dessus, pour voir les détails de chaque session **Facebook** que vous avez pu oublier de déconnecter – par exemple dans un cybercafé ou sur l'ordinateur d'un ami – et qui donc est encore active.

**Active Sessions**

**Current Session**  
**Location:** Berlin, BE, DE (Approximate)  
**Device Type:** Firefox on Linux

---

If you notice any unfamiliar devices or locations, click 'End Activity' to end the session. This list does not currently include sessions on Facebook's mobile site (m.facebook.com).

---

**Last Accessed: June 4 at 12:48pm** [End Activity](#)  
**Location:** Berlin, BE, DE (Approximate)  
**Device Type:** Unknown [?]

---

**Last Accessed: June 4 at 12:48pm** [End Activity](#)  
**Location:** Berlin, BE, DE (Approximate)  
**Device Type:** Unknown [?]

---


**Last Accessed: June 3 at 2:49pm** [End Activity](#)  
**Location:** Berlin, BE, DE (Approximate)  
**Device Type:** Chrome on WinXP

Graphique 14 : Exemple d'une liste de plusieurs sessions actives

Il est très important de fermer ces sessions afin d'empêcher quiconque d'accéder à votre compte **Facebook**, surtout si vous remarquez des appareils dans la liste qui ne vous appartiennent pas ou que vous ne reconnaissez pas. Pour ce faire, il suffit de **cliquer** sur *Fin de session* à côté de chaque session active.

## 2.3 Abonnés

**Facebook** vous donne la possibilité d'autoriser des gens à **s'abonner** à votre fil d'actualités sans que vous soyez amis. Sachez toutefois que si vous permettez à d'autres de s'abonner à votre fil d'actualités, certaines de vos données leur seront alors disponibles ainsi qu'aux membres de leurs réseaux. L'option la plus sûre est de ne pas permettre aux gens de s'abonner à votre fil d'actualités.

**Étape 16.** Cliquez sur l'onglet  à gauche suivant le *Graphique 7* ci-dessus et assurez-vous que la case *Autoriser les abonnés* n'est pas cochée.

**Autoriser les abonnés**  Les abonnés recevront vos publications avec le paramètre Public et ne seront pas ajoutés à votre liste d'amis. Vous pouvez désormais séparer vos conversations entre amis de celles pour une audience plus large. [En savoir plus.](#)

---

[Vous voulez savoir ce que les abonnés peuvent voir ? Consultez la version publique de votre journal.](#)


Graphique 15 : Paramètres d'abonnement

## 2.4 Paramètres des applications

Beaucoup de gens utilisent des *applications (apps)* tierces tels des jeux ou des social readers interagissant avec leur compte **Facebook**.

Pour utiliser un grand nombre de ces apps, il vous faudra consentir à permettre aux propriétaires de ces apps de voir certaines informations vous concernant vous **et vos amis**, qui pourraient inclure des informations personnelles telles que l'âge, l'emplacement, la scolarité, l'état civil, les opinions religieuses et politiques, l'état des mises à jour, les informations de contact et bien d'autres choses. Afin de protéger au mieux votre vie privée ainsi que celle de vos amis et contacts, nous vous recommandons de **ne pas utiliser d'applications tierces** sur **Facebook**, à moins d'être sûr de leur intégrité.


Les apps peuvent être désinstallées :

**Étape 17.** Cliquez sur l'onglet  Applications dans la barre à gauche. Vous verrez alors la liste des apps actuellement liées à votre profil.

 BranchOut	Il y a moins de 24 heures	<a href="#">Modifier</a> 
 Dr. Sketchy's Anti-Art School	25 octobre	<a href="#">Modifier</a> 
 Spotify	Il y a plus de six mois	<a href="#">Modifier</a> 
 The Food List Challenge	Il y a plus de six mois	<a href="#">Modifier</a> 
 The World Traveler Challenge	Il y a plus de six mois	<a href="#">Modifier</a> 

Graphique 16 : Exemple d'une liste d'applications

**Étape 18.** Cliquez sur l'application que vous souhaitez supprimer de la liste.

 Spotify Dernière connexion : Il y a plus de six mois [Supprimer l'application](#)

---

Cette application a besoin de :

- Votre adresse électronique
- Votre anniversaire
- Permission d'accéder à vos données lorsque vous n'êtes pas en ligne

Graphique 17 : Un clic sur une application dans la liste permet d'afficher les informations que vous avez mises à la disposition des propriétaires de l'app

Étape 19. Cliquez *Supprimer l'application* en haut à droite du menu déroulant.

## Comment mettre à jour vos paramètres de confidentialité

Liste des sections de cette page :

- [3.1 Prise de contact](#)
- [3.2 Journal et identification](#)
- [3.3 Applications et sites web](#)
- [3.4 Publicités](#)

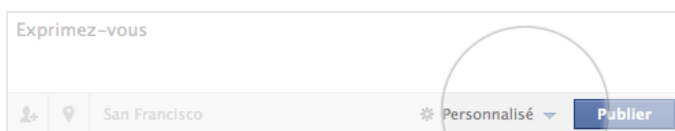
**Facebook** a de plus en plus permis à ses utilisateurs de garder le contrôle sur certains aspects de leur vie privée. Si l'on examine ces options, on s'aperçoit qu'il est possible d'atteindre un niveau convenable de confidentialité sur **Facebook**.

Pour modifier vos paramètres de confidentialité sur **Facebook**, **sélectionnez** *Paramètres de confidentialité* dans le menu déroulant situé en haut à droite de la page. Vous accédez ainsi à la page *Paramètres de confidentialité* où il est recommandé de **sélectionner** le bouton *Personnalisé* afin d'être sûr d'avoir le contrôle complet sur ses paramètres de confidentialité.

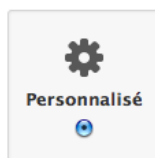
### Contrôler la confidentialité de ce que vous publiez

Vous pouvez gérer la confidentialité de vos mises à jour de statut, photos et informations avec le sélecteur d'audience, lorsque vous publiez ou par la suite. N'oubliez pas – les personnes qui peuvent voir ce que vous publiez peuvent également partager ce contenu avec d'autres personnes, y compris les applications. [En savoir plus.](#)

Le paramètre de confidentialité de votre prochaine publication est actuellement : \* Personnalisé :



L'option que vous sélectionnez est celle retenue pour votre prochaine publication. Mais vous pouvez la changer au moment de publier ou ici :



### **Prise de contact**

Contrôler la prise de contact avec les personnes que vous connaissez.

[Modifier les paramètres](#)

### **Journal et identification**

Contrôlez ce qui se produit lorsque des amis vous identifient, identifient votre contenu ou publient sur votre journal.

[Modifier les paramètres](#)

### **Publicités, applications et sites web**

Gérez vos paramètres pour les publicités, applications, jeux et sites web.

[Modifier les paramètres](#)

### **Limiter la visibilité des anciennes publications**

Limiter l'audience des publications que vous avez ouvertes aux amis de vos amis ou au public.

[Gérer la visibilité des anciennes publications](#)

### **Personnes et applications bloquées**

Gérer les personnes et les applications que vous avez bloquées.

[Gérer le blocage](#)

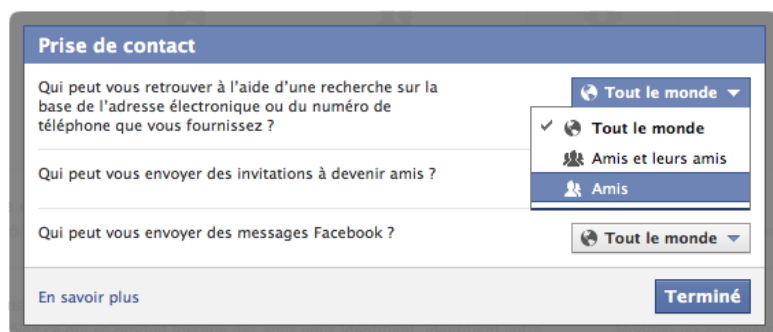
Graphique 1 : page *Paramètres de confidentialité*

## 3.1 Prise de contact

La première section à éditer s'intitule « *Prise de contact* » où vous pouvez définir les personnes qui peuvent voir votre profil, vous envoyer des messages ou vous ajouter comme ami.

Étape 1. Cliquez sur *Modifier les paramètres* dans l'onglet *Prise de contact*.

**Étape 2.** Choisissez pour chaque point le paramètre « Amis » afin que votre réseau ne soit accessible que par le petit groupe de personnes que vous connaissez, et non par tout le monde :



Graphique 2 : Options Prise de contact

## 3.2 Journal et identification

Dans le menu *Journal et identification*, vous pouvez déterminer ce qui se produit lorsque des amis vous identifient, identifient votre contenu ou publient sur votre journal.

**Étape 3.** Cliquez sur le menu *Journal et identification*. Des options protectives supplémentaires apparaîtront en bas du menu déroulant :



Graphique 3 : Menu Journal et identification

**Étape 4.** Choisissez si vous souhaitez ou non que vos amis ou contacts puissent publier sur votre journal.

**Note** Si vous décidez de permettre à vos amis et contacts de publier sur votre journal, vous pouvez également faire en sorte que ces publications ne soient vues que par vous. Pour ce faire, **sélectionnez** le bouton *Personnalisé* dans la ligne *Qui peut voir ce que d'autres personnes publient sur votre journal*, puis dans l'option *Montrer à ces personnes : moi uniquement*.

**Étape 5.** Activer l'*examen du journal* qui vous permet de contrôler et d'approuver les publications et photos dans lesquelles on vous mentionne avant leur apparition sur votre journal. Vous pouvez ainsi vérifier que vos amis ou votre famille ne dévoilent pas votre emplacement ou des détails personnels.

**Facebook** a commencé à utiliser une technologie de **reconnaissance faciale** qui lui permet de vous identifier dans des photos postées par vos amis et 'contacts' et de leur suggérer de vous *identifier* sur leurs photos. Pour tout défenseur des droits de l'homme, il s'agit d'un thème sensible et il est donc recommandé de désactiver cette option.

**Étape 6.** Cliquez sur *Qui voit les suggestions d'identification lorsque vous semblez apparaître dans une photo téléchargée* et **sélectionnez** *Personne*.





Graphique 4 : Options Qui voit les suggestions d'identification

**Étape 7. Cliquez** Terminé

**Facebook** vous permet également de faire « disparaître » d'anciennes publications de votre journal après un certain laps de temps.

**Étape 8. Cliquez** sur *Gérer la visibilité des anciennes publications* dans l'onglet *Limiter la visibilité des anciennes publications*.



Graphique 5 : Option Visibilité d'anciennes publications

**Étape 9. Cliquez** sur "Limiter la visibilité des anciennes publications".



Graphique 6 : Option Limiter la visibilité des anciennes publications




**Étape 10. Cliquez** Confirmer

### 3.3 Applications et sites web

Comme il est mentionné dans la section 2.4 de ce présent chapitre, de nombreuses applications sur **Facebook** nécessitent non seulement l'accès aux informations de l'utilisateur mais aussi à celles de ses amis. Il est donc possible que des tierces parties soient en mesure de collecter des informations vous concernant alors que vous-même n'utilisez

pas d'applications mais parce que des amis le font. Toutefois, ce n'est pas une fatalité. Pour empêcher des amis de partager vos informations privées par le biais des applications qu'ils utilisent :

**Étape 11.** Cliquez sur *Publicités, applications et sites web* et cliquez sur les paramètres *Comment les autres transmettent vos informations aux applications qu'ils utilisent* :

<b>Applications que vous utilisez</b>	Vous utilisez 5 applications, jeux et sites web dernièrement :  <b>BranchOut</b> Il y a moins de 24 heures  <b>Dr. Sketchy's Anti-Art School</b> 25 octobre  Désactiver la possibilité d'utiliser des applications, des modules et des sites web sur et en dehors de Facebook. Lorsque vous désactivez cette option, nous n'enregistrons plus d'informations concernant votre utilisation d'applications ou de sites web en dehors de Facebook.	<a href="#">Modifier les paramètres</a>
<b>Anciennes versions d'applications mobiles Facebook</b>	Ce paramètre contrôle la confidentialité de ce que vous publiez avec d'anciennes applications mobiles de Facebook qui n'ont pas de sélecteur d'audience (c'est le cas pour Facebook pour BlackBerry, par exemple).	<a href="#">Amis et leurs amis</a>
<b>Comment les autres transmettent vos informations aux applications qu'ils utilisent</b>	Vos amis ont accès à vos informations et peuvent les utiliser lorsqu'ils utilisent des applications. Utilisez ce paramètre pour contrôler quelles catégories vos amis peuvent utiliser.	<a href="#">Modifier les paramètres</a>
<b>Personnalisation instantanée</b>	Vous permet de voir des informations liées à vos amis dès que vous arrivez sur certains sites web partenaires.	<a href="#">Modifier les paramètres</a>
<b>Recherche publique</b>	Afficher un aperçu de votre journal Facebook dans les résultats des moteurs de recherche.	<a href="#">Modifier les paramètres</a>
<b>Publicités</b>	Gérer les paramètres pour les publicités sociales et de tiers.	<a href="#">Modifier les paramètres</a>

Graphique 7 : Options Applications, jeux et sites web

Il est recommandé de décocher toutes les cases afin d'assurer la protection complète de vos données et qu'elles ne puissent être ni trouvées ni utilisées par des applications tierces que vos amis utilisent. Ensuite cliquez sur

[Enregistrer les modifications](#)

**Comment les autres transmettent vos informations aux applications qu'ils utilisent**

Vos amis ont accès à vos informations et peuvent y avoir accès lorsqu'ils utilisent une application. Cela leur permet d'avoir une meilleure expérience sociale. Utilisez le paramètre ci-dessous pour contrôler les catégories d'information que vos amis peuvent utiliser lorsqu'ils utilisent des applications, des jeux ou des sites.

<input type="checkbox"/> Bio	<input type="checkbox"/> Mes vidéos
<input type="checkbox"/> Date de naissance	<input type="checkbox"/> Mes liens
<input type="checkbox"/> Famille et relations	<input type="checkbox"/> Mes articles
<input type="checkbox"/> Intéressé(e) par	<input type="checkbox"/> Ville d'origine
<input type="checkbox"/> Opinions politiques et religieuses	<input type="checkbox"/> Ville actuelle
<input type="checkbox"/> Mon site web	<input type="checkbox"/> Formation et emploi
<input type="checkbox"/> Si je suis en ligne	<input type="checkbox"/> Activités, intérêts, choses que j'aime
<input type="checkbox"/> Mes statuts	<input type="checkbox"/> Mon activité liée aux applications
<input type="checkbox"/> Mes photos	

Si vous ne souhaitez pas que les applications et sites web puissent accéder à d'autres catégories d'information (comme votre liste d'amis, votre sexe ou les infos avec le paramètre Public), vous pouvez désactiver toutes les applications de la plate-forme. N'oubliez pas cependant que vous ne pourrez plus utiliser de jeux ou d'applications.

[Enregistrer les modifications](#)
[Annuler](#)

Graphique 8 : Options Comment les autres transmettent vos informations aux applications qu'ils utilisent

La *personnalisation instantanée* de **Facebook** accorde également à certains sites l'accès aux informations liées à votre profil public lorsque vous allez sur ces sites. Ces sites adaptent leur contenu web en fonction de vos souhaits et besoins, créant ainsi une expérience personnalisée. Pour plus de sécurité, désactivez ce service s'il est disponible dans votre région.

**Étape 12.** Cliquez [Modifier les paramètres](#) dans l'onglet *Personnalisation instantanée*. Cliquez [Terminé](#) sur l'écran qui apparaît et qui explique ce qu'est une *Personnalisation instantanée*, et assurez-vous que la case *Activez la personnalisation sur les sites web partenaires*, en bas de la prochaine page, n'est pas cochée.

◀ Revenir aux applications

**Personnalisation instantanée**

Nous nous sommes associés à quelques sites web pour vous fournir une expérience plus personnalisée dès que vous arrivez sur ces sites comme, par exemple, commencer à jouer la musique que vous aimez ou vous montrez des critiques publiées par vos amis. Ces partenaires ont accès aux informations publiques par défaut (comme votre nom et la photo de votre profil) et à celles auxquelles vous avez appliqué le paramètre Public.

Lorsque vous arriverez pour la première fois sur les sites suivants, vous verrez un message d'information et une option vous permettant de désactiver l'expérience personnalisée :

- Bing – Moteur de recherche
- Pandora – Musique personnalisée
- TripAdvisor – Voyage social
- Yelp – Avis de vos amis
- Rotten Tomatoes – Avis d'amis sur les films
- Clicker – Recommandations télévisuelles personnalisées
- Scribd – Lecture sociale
- Docs – Documents en collaboration
- Zynga – Social Games (The Ville, Zynga Slingo and 11 autres jeux)
- Kixeye – Jeux de société (War Commander et Battle Pirates)
- EA – Social Games (SimCity Social)

Pour désactiver la personnalisation instantanée sur tous les sites partenaires, il vous suffit de désactiver l'option ci-dessous.

Activer la personnalisation instantanée sur les sites web partenaires.

Figure 9: Options Personnalisation instantanée

Une des meilleures façons de trouver des informations sur quelqu'un consiste simplement à entrer son nom dans un moteur de recherche tel que **Google**. Pour éviter que des adversaires trouve votre page **Facebook** aussi facilement, pensez à ne pas non plus être visible dans les moteurs de recherche publics tels que **Google, Bing, Yahoo**, etc.

**Étape 13.** Cliquez *Modifier les paramètres* dans l'onglet *Recherche publique* et décochez la case à côté de *Activer le jour de mes 18 ans*.

◀ Revenir aux applications

**Recherche publique**

La recherche publique contrôle également si un aperçu de votre journal Facebook sera affiché dans les résultats de recherche lorsque quelqu'un entre votre nom dans un moteur de recherche. Certains moteurs de recherche conservent un « cache » (une sorte de copie de sauvegarde) et les informations de votre journal peuvent donc rester disponibles pendant un certain temps après que vous avez désactivé le paramètre de recherche publique. Remarque – Cette fonctionnalité n'est pas disponible si vous avez moins de 18 ans. [En savoir plus](#)

Pour utiliser cette fonctionnalité, accédez d'abord à [Prise de contact](#) et réglez Qui peut trouver votre journal en cherchant votre nom ? sur Tout le monde.

Activer le jour de mes 18 ans

Graphique 10 : Options Recherche publique

**Étape 14.** Cliquez **Confirmer** si cela vous est demandé.

### 3.4 Publicités

**Publicités de Facebook:** Facebook s'engage actuellement à ne pas associer votre nom ou photo à des publicités de tierces parties, toutefois une marge de manoeuvre rendant cela possible à l'avenir a été conservée. En cas de futur changement des règles sur la publicité, il est donc conseillé de changer ses paramètres de façon à ce que vos détails restent confidentiels :



Graphique 11 : Options publicités

Étape 15. Cliquez sur *Modifier les paramètres* dans l'onglet *Publicités*.

Étape 16. Cliquez *Modifier les paramètres de publicités tierces* dans *Publicités diffusées par des tiers*.

Étape 17. Dans le menu déroulant à côté de *Si nous l'autorisons à l'avenir, montrer mes informations à* : **sélectionnez** *Personne*.

Étape 18. Cliquez **Enregistrer les modifications**.

Étape 19. Dans *Publicités et les amis*, cliquez *Modifier les paramètres des publicités sociales*.

Étape 20. En bas de la page, à côté de *Associer mes actions sociales avec les publicités pour* : **sélectionnez** *Personne*.

Étape 21. Cliquez **Enregistrer les modifications**.

## Comment désactiver ou supprimer votre page Facebook

Liste des sections de cette page :

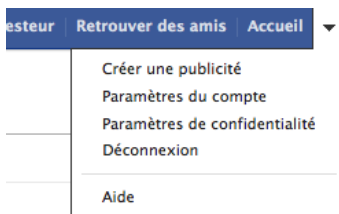
- [4.1 Désactivation de votre compte Facebook](#)
- [4.2 Suppression de votre compte Facebook](#)

### 4.1 Désactivation de votre compte Facebook

Vous pouvez envisager de désactiver votre compte **Facebook** à chaque fois que vous vous déconnectez et de le réactiver lorsque vous souhaitez l'utiliser. Ainsi, votre page **Facebook** et les informations de votre profil seront inaccessibles à d'autres utilisateurs, vos amis inclus, lorsque vous n'êtes pas en ligne. Mais vos informations n'ont pas pour autant été supprimées et sont réaccessibles dès que vous vous connectez.

Pour désactiver votre page **Facebook** :

Étape 1. **Sélectionnez** *Paramètres du compte* dans le menu déroulant en haut à droite de l'écran.



Graphique 1: Menu Paramètres

Étape 2. Cliquez sur  *Sécurité* dans le menu à gauche.

**Étape 3. Facebook** va vous montrer une page dans le but de vous convaincre de ne pas désactiver votre profil, contenant un court questionnaire quant aux raisons pour lesquelles vous souhaitez désactiver. L'important à savoir ici est que si vous êtes le seul administrateur d'une *page* ou *groupe Facebook* (p.ex. pour une organisation ou une campagne) et que vous ne souhaitez pas que ceux-ci soient fermés alors que votre compte est désactivé, vous devrez nommer un autre administrateur.



Raison de votre départ (obligatoire) :

- Je passe trop de temps sur Facebook.
- Je ne trouve pas Facebook utile.
- Je ne sais pas comment utiliser Facebook.
- J'ai un souci de confidentialité.
- Mon compte a été piraté.
- J'ai un autre compte Facebook.
- Je ne me sens pas en sécurité sur Facebook.
- Je reçois trop de messages électroniques, d'invitations et de demandes de la part de Facebook.
- C'est temporaire. Je reviendrai.
- Autre

Veillez expliquer plus précisément :

Refus de messages électroniques :  Ne plus recevoir de messages de la part de Facebook

Remarque – même après la désactivation de votre compte, vos amis peuvent toujours vous inviter aux événements, vous identifier sur des photos ou vous inviter à rejoindre des groupes. Si vous refusez, vous ne recevrez PAS les messages électroniques d'invitation et de notification de vos amis.

Graphique 2 : Confirmer que vous souhaitez désactiver votre page

**Étape 4.** Cliquez sur  en bas de la page.

**Étape 5.** Entrez votre mot de passe et cliquez sur

**Étape 6.** Tapez les nombres et lettres aléatoires dans l'encadré pour le contrôle de sécurité et cliquez sur .

## 4.2 Suppression de votre compte Facebook

Après la désactivation de votre profil **Facebook**, vous pouvez revenir et réaccéder à toutes vos informations simplement en vous connectant. Toutefois, si vous ne souhaitez pas continuer à utiliser **Facebook**, vous pouvez de fait supprimer votre profil complet. Sachez que vous n'aurez plus accès aux informations que vous avez stockées sur votre compte **Facebook** tels des photos ou des messages. Quoi qu'il en soit, vous pouvez télécharger une copie de ces informations avant de supprimer votre profil.

**Étape 1.** Allez à l'adresse [https://www.facebook.com/help/delete\\_account](https://www.facebook.com/help/delete_account)



**Supprimer mon compte**

Si vous ne pensez jamais réutiliser Facebook et souhaitez effacer complètement votre compte, nous pouvons nous en charger. Rappelez-vous cependant que vous ne pourrez ni réactiver votre compte ni récupérer son contenu ou ses informations. Si vous souhaitez tout de même supprimer votre compte, cliquez sur Supprimer mon compte.

Graphique 3 : Supprimer la page de votre profil

**Étape 2.** Cliquer sur .

**Étape 3.** Tapez votre mot de passe et les nombres ou lettres aléatoires pour le contrôle de sécurité.



Graphique 4 : Contrôle de sécurité final

**Étape 4.** Cliquez sur **OK**. Un message apparaîtra, indiquant que votre compte sera supprimé dans 14 jours. Durant cette période, vous pourrez toujours encore réactiver votre compte, ce qui annulera votre décision de le supprimer.

Vous pouvez également supprimer votre compte via e-mail, en envoyant un courriel à [privacy@facebook.com](mailto:privacy@facebook.com) leur demandant de supprimer votre compte.

**Note Facebook** ne précise pas si vos informations sont définitivement supprimées de leur base de données. Et les autorités peuvent toujours demander ces informations à Facebook. En outre, la suppression ne concerne que l'information directement liée à votre compte. Des informations liées à certaines de vos activités sur Facebook - comme publier sur la page d'un groupe ou envoyer un message, ne seront pas supprimées.

## Guide de sécurisation de Twitter

**Twitter** est un réseau social dans lequel les gens partagent des informations via des *mises à jour de statut* limitées à 140 caractères. Ces mises à jour répondaient initialement à la question « Que faites-vous maintenant? ». Il est depuis devenu un moyen de diffusion de différents types d'information. La différence avec **Facebook** est que sur **Twitter**, vous 'suivez' d'autres utilisateurs qui vous intéressent, plutôt que des gens que vous connaissez réellement.

### Page d'accueil

- [www.twitter.com](http://www.twitter.com) <sup>[254]</sup>

### Configuration de l'ordinateur

- Une connexion Internet
- [Navigateur web Firefox avec des extensions de sécurité](#) <sup>[247]</sup> ou [Navigateur web Tor](#) <sup>[248]</sup>

### Lecture obligatoire

- Livret pratique chapitre **10. Savoir se protéger sur les sites de réseautage social** <sup>[255]</sup>
- Les [Conditions d'utilisation](#) <sup>[256]</sup> et la [politique de confidentialité](#) <sup>[257]</sup> de **Twitter**

**Temps nécessaire pour commencer à utiliser cet outil** : 40 minutes

### Ce que vous obtenez en retour:

- L'aptitude à **réduire** la quantité d'informations personnelles rendues publiques lors de votre utilisation de Twitter
- L'aptitude à **contrôler** qui peut voir vos mises à jour, photos et autres données partagées sur Twitter
- L'aptitude à **réduire** la quantité d'informations personnelles accessibles à des tierces parties.

### 1.1 Ce qu'il faut savoir sur cet outil avant de commencer

**Twitter** déclare dans ses conditions d'utilisation : « Cette licence signifie que vous nous autorisez à mettre vos tweets à la disposition du reste du monde et que vous permettez aux autres d'en faire de même. (...) Mais ce qui vous appartient vous appartient – vous restez propriétaire de vos Contenus ». Toutefois, **Twitter** se réserve le droit de transmettre vos informations aux gouvernements qui en font la demande.

Bien que **Twitter** soit un site web, beaucoup de gens interagissent avec et gèrent **Twitter** depuis des applications pour ordinateur et smartphone appelées clients **Twitter**. Si vous utilisez un client **Twitter**, vous devez vous assurer qu'il est correctement connecté au site, via une connexion chiffrée. Pour cela, consultez [Sécuriser votre courriel](#) <sup>[258]</sup> dans le **chapitre 7 : Préserver la confidentialité de vos communications sur Internet** <sup>[126]</sup>.

En outre, comme pour **Facebook**, beaucoup de gens utilisent **Twitter** en conjonction avec de nombreux autres sites web et applications pour partager des mises à jour de statut, des photos, des lieux, des liens, et ainsi de suite. L'utilisation de ces applications implique de nombreuses failles de sécurité potentielles et il est très important de sécuriser les paramètres de confidentialité des autres applications autant que possible.

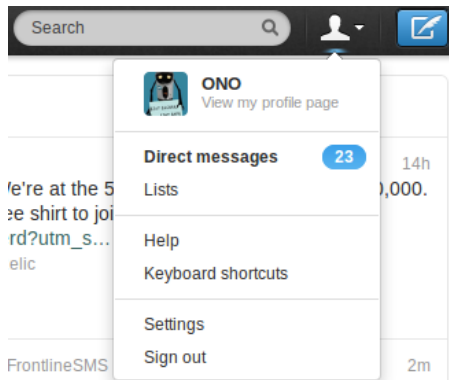
Le département de la Sécurité intérieure des États-Unis surveille **Twitter** et d'autres sites de réseautage social, et il est fort probable que d'autres gouvernements en font de même.

Pour plus d'informations sur la [politique de confidentialité](#) <sup>[259]</sup> de **Twitter**, consultez ces infographies sur le site **Me**

# Comment modifier les paramètres généraux du compte Twitter

## 2.1 Paramètres généraux du compte Twitter

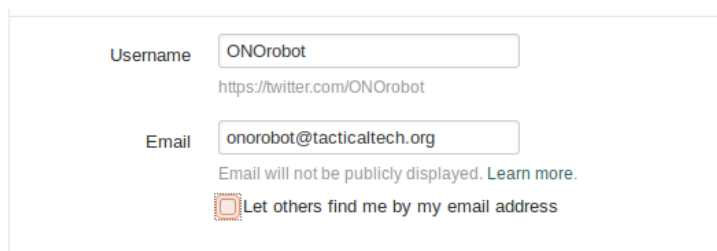
Les paramètres généraux du compte **Twitter** vous permettent entre autres de contrôler la façon dont les gens peuvent découvrir votre profil, qui peut voir vos tweets, les informations de localisation que vous donnez lorsque vous utilisez la version web de **Twitter** (et non une version client, une application pour smartphones ou un téléphone mobile).



Graphique 1 : Options

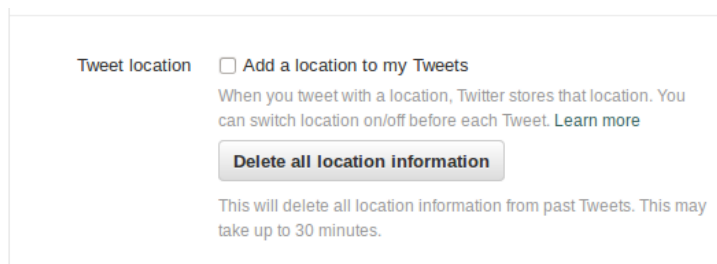
**Étape 1.** Cliquez sur l'icône en haut à droite de l'écran et **sélectionnez Paramètres**. La page des paramètres apparaîtra.

**Étape 2.** En haut de la liste des paramètres du compte, vous trouverez les paramètres Nom d'utilisateur et Adresse email. Décidez soigneusement si vous comptez utiliser votre vrai nom ou un pseudonyme en tant que **nom d'utilisateur** et quelle adresse électronique vous souhaitez associer à votre profil. **Décochez** la case intitulée *Permettre de me trouver grâce à mon adresse email*.



Graphique 2: Paramètres Nom d'utilisateur et Adresse email

**Étape 3.** **Twitter** vous propose l'option d'inclure votre localisation dans vos tweets. Ceci implique un certain nombre de conséquences quant à la sécurité : par exemple, si vous êtes loin de la ville où vous habitez, vous donnez une indication utile à des adversaires potentiels qui souhaitent s'introduire sans surveillance chez vous ou dans votre bureau, ou pire. Par conséquent, assurez-vous que la case *Ajouter une localisation à mes tweets* est **décochée**.



Graphique 3 : Options localisation

**Étape 4.** Cliquez sur **Delete all location information** pour que toutes les informations liées à votre localisation soient supprimées de vos prochains tweets.

**Étape 5.** Les paramètres par défaut sur **Twitter** font que tous vos tweets peuvent être vus par tout le monde, y compris par des gens qui ne vous suivent pas ou qui n'ont pas même de compte **Twitter**. De nombreux, voire tous les gouvernements contrôlent ce qui se passe sur **Twitter**, et on répertorie un nombre croissants d'incidents dans lesquels des défenseurs des droits de l'homme ont été persécutés à cause du contenu de leurs tweets. Par conséquent, il est fortement recommandé de **sélectionner Protéger mes tweets** afin que seuls les utilisateurs qui vous suivent puissent voir vos tweets, et que vous puissiez approuver personnellement ceux qui y ont accès. Toutefois, il convient de garder à l'esprit que la politique de confidentialité de **Twitter** énonce qu'ils peuvent transmettre des informations aux autorités légales si celles-ci en font la demande.

Tweet privacy  Protect my Tweets  
If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. [Learn more.](#)

Graphique 4 : Options Protéger mes tweets

**Étape 6.** Twitter propose un service de *personnalisation* qui surveille vos mouvements de navigation sur tous les sites web incluant un bouton ou widget **Twitter** et, à partir de ces mouvements, il vous suggère de suivre des gens ou des organisations. Si ce service est disponible, il est recommandé de le **désactiver** et en outre d'utiliser la fonction **DoNotTrack** <sup>[261]</sup> dans le navigateur Firefox afin d'augmenter votre confidentialité en ligne.

**Étape 7.** Twitter vous permet d'utiliser une connexion **Secure Socket Layer (SSL)** chiffrée et sécurisée (aussi appelée « HTTPS »), qui empêche qui que ce soit d'« épier » la communication entre votre ordinateur et le site de **Twitter**. Assurez-vous que *Toujours utiliser HTTPS* est **coché**.

HTTPS only  Always use HTTPS  
Use a secure connection where possible.

Graphique 5 : Options HTTPS

**Note:** Rappelez-vous que ce paramètre ne s'applique que lorsque vous utilisez **Twitter** à partir de votre navigateur web, tel que Firefox. Si vous utilisez un **client Twitter** tel que **HootSuite** ou une application pour smartphones, il vous faudra modifier les paramètres dans le client ou l'application afin d'établir une connexion SSL, et cette option **n'est pas disponible pour tous les clients ou applications**.

**Étape 8.** Cliquez sur

Save changes

## Clients et applications Twitter

Liste des sections de cette page:

- [2.0 Indications générales sur les clients et les applications](#)
- [2.1 TwitPic](#)
- [2.2 YFrog](#)
- [2.3 HootSuite](#)
- [2.4 Applications pour smartphones](#)

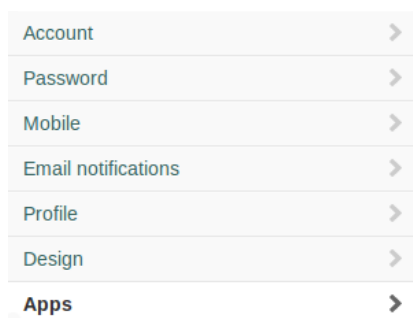
---

## 2.0 Indications générales sur les clients et les applications

Les utilisateurs de **Twitter** peuvent permettre à diverses applications de tierces parties, y compris d'autres sites de réseautage social et de partage de photos, d'interagir avec leur compte **Twitter**, pour par exemple partager des photos téléchargées via des sites tels que **TwitPic**, **YFrog** ou **Flickr**. Toutefois, comme il est mentionné dans le chapitre **10**, **Savoir se protéger sur les sites de réseautage social** <sup>[239]</sup>, soyez prudent lors que vous intégrez votre profil sur différents sites de réseautage social. Ces sites de tierces parties ont leurs propres conditions d'utilisation, politiques de confidentialité et paramètres de confidentialité et celles-ci ne sont pas nécessairement les mêmes que sur **Twitter**. Par conséquent, même si votre compte **Twitter** est relativement sûr, votre profil peut être complètement visible sur les sites d'applications de tierces parties et si vous utilisez le même nom d'utilisateur ou adresse électronique, vous pouvez être facilement retrouvable. Ces sites et applications sont très nombreux et seuls quelques-uns sont présentés dans ce guide. Quoi qu'il en soit, il est essentiel que vous recherchiez et mettiez à jour vos paramètres de sécurité pour chaque application de tierce partie liée à votre compte **Twitter**. Si vous ne les considérez pas comme assez sûres, supprimez votre profil et révoquez son accès à votre compte **Twitter**.

Si vous souhaitez révoquer l'accès d'une application à votre profil **Twitter** :

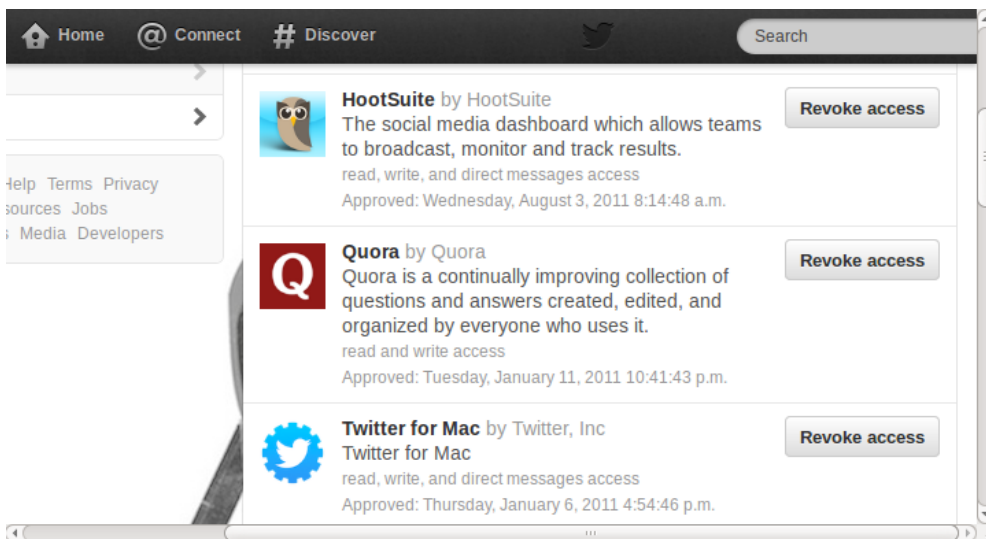
**Étape 1.** Allez dans les *paramètres* de votre compte et **cliquez** l'onglet *Applications* situé à gauche.



Graphique 1 : Menu Paramètres

**Étape 2.** Vous avez ouvert la liste des apps connectées à votre compte **Twitter**, **sélectionnez** l'application dont vous voulez révoquer l'accès, cliquez sur **Revoke access**.





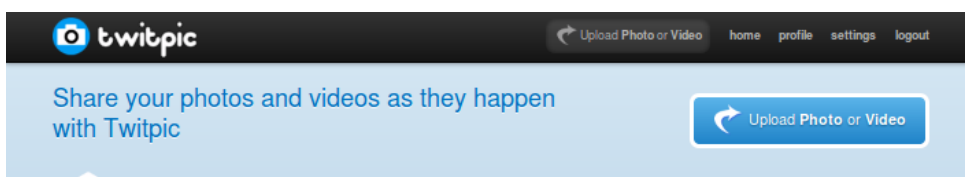
Graphique 2 : Un exemple de liste d'applications

## 2.1 TwitPic

Beaucoup d'utilisateurs de **Twitter** utilisent également le site **TwitPic** pour télécharger et stocker des photos qu'ils partagent via **Twitter**. Gardez à l'esprit que **TwitPic** est une entreprise distincte qui n'appartient pas à **Twitter** et que ses conditions d'utilisation tout comme sa politique de confidentialité ne sont pas les mêmes que sur Twitter. À cet égard, il est important de noter que **TwitPic ne donne pas** à ses utilisateurs la possibilité de cacher leur profil ou leurs photos. Toutes les photos téléchargées sur **TwitPic** sont publiques par défaut et cela ne peut pas être changé. Si vous utilisez le même nom d'utilisateur pour **Twitter** et **TwitPic**, un adversaire accèdera très facilement à toutes les photos que vous avez téléchargées sur **TwitPic**.

**TwitPic** permet aux autres utilisateurs de vous taguer dans les photos qu'ils prennent. Vous courez un risque potentiel si l'on vous tague dans une photo sensible, étant donné que cette information sera rendue publique. Par conséquent, il est recommandé d'interdire aux autres utilisateurs de vous taguer dans leurs photos.

**Étape 1.** Cliquez sur *Paramètres* dans le menu en haut à droite de l'écran.



Graphique 3 : La barre de menu sur la page d'accueil de TwitPic

**Étape 2.** Dans *privacy* (confidentialité), **décochez** la case intitulée *Allow others to tag my photos* (permettre aux autres de taguer mes photos) et **cliquez** sur le bouton *Save Changes* (enregistrer les modifications).

### Privacy

Show my updates in the public timeline

Allow others to tag my photos

Save Changes

Graphique 4 : Options Tag

Si vous souhaitez supprimer des photos sensibles de **TwitPic**:

**Étape 3.** Cliquez *Profile* dans le menu en haut à droite de l'écran.

**Étape 4.** Cliquez *Delete* (supprimer) à côté des photos que vous souhaitez supprimer.



about a minute ago via site 0

delete

1

Graphique 5 : Options Image

Si vous souhaitez supprimer votre compte **TwitPic**.


**Étape 5.** Cliquez *Settings* (paramètres) dans le menu en haut à droite de l'écran.

**Étape 6.** Dans la section *Delete Account* (supprimer le compte), tapez les mots du « captcha » dans l'encadré.

## Delete Account

If you would like to delete your account, you may do so here. Enter the captcha first to continue.

Graphique 6 : Ce « captcha » apparaît avant que vous puissiez supprimer votre profil

**Étape 7.** Cliquez sur .

## 2.2 YFrog

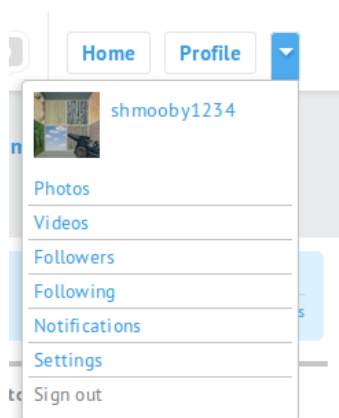
**YFrog** appartient à la corporation **ImageShack**

Au moment de la rédaction de ce présent guide, toutes les photos téléchargées sur **YFrog** sont publiques par défaut, comme c'est le cas sur **TwitPic**, et il n'y a aucun moyen de changer cela. Selon les conditions d'utilisation d'ImageShack, vous pouvez révoquer leur droit de publier vos contenus en les contactant directement. La mise en vigueur de cette demande peut prendre jusqu'à 24 heures.

Toutefois, si vous protégez vos tweets sur **Twitter**, ceux-ci ne seront pas visibles dans votre compte **YFrog**. Vos photos par contre le seront toujours.

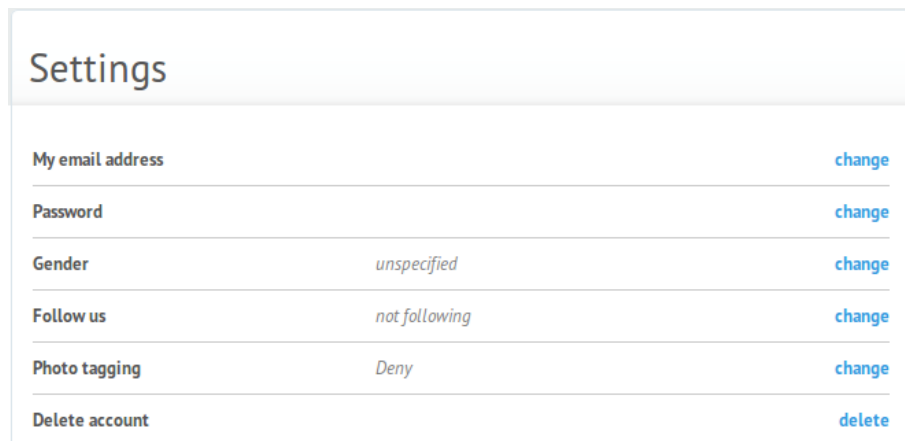
**YFrog** permet aux autres utilisateurs de vous taguer dans les photos qu'ils prennent. Vous courez un risque potentiel si l'on vous tague dans une photo sensible, étant donné que cette information sera rendue publique. Par conséquent, il est recommandé d'interdire aux autres utilisateurs de vous taguer dans leurs photos.

**Étape 1.** Cliquez sur l'écrou en haut à droite de l'écran et sélectionnez *Settings* (paramètres)



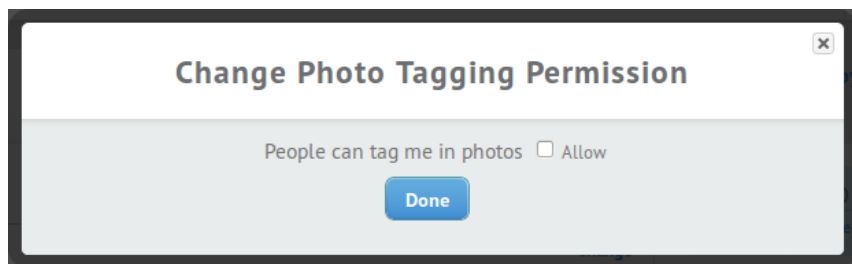
Graphique 7 : Options YFrog

Ceci vous mènera à la page des paramètres d'YFrog.



Graphique 8 : Le menu des paramètres sur YFrog.


**Étape 2.** Sous Photo tagging (comme dans l'image ci-dessous), **cliquez** sur *Change* et **décochez** la case intitulée *People can tag me in their photos* (les gens peuvent me taguer dans leurs photos).



Graphique 9 : Options Photo tagging

Si vous souhaitez supprimer votre compte **YFrog**, retournez dans le menu *Settings* (paramètres) :

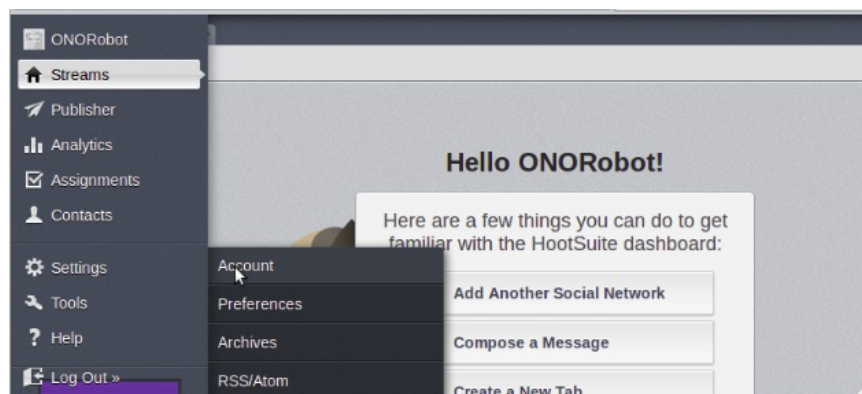
**Étape 3.** Sur la page des paramètres, **cliquez** sur *Delete* (supprimer) à côté de l'option *Delete account* (supprimer le compte). Vous serez invité à saisir votre mot de passe.

**Étape 4.** Tapez votre mot de passe et cliquez sur .

## 2.3 HootSuite

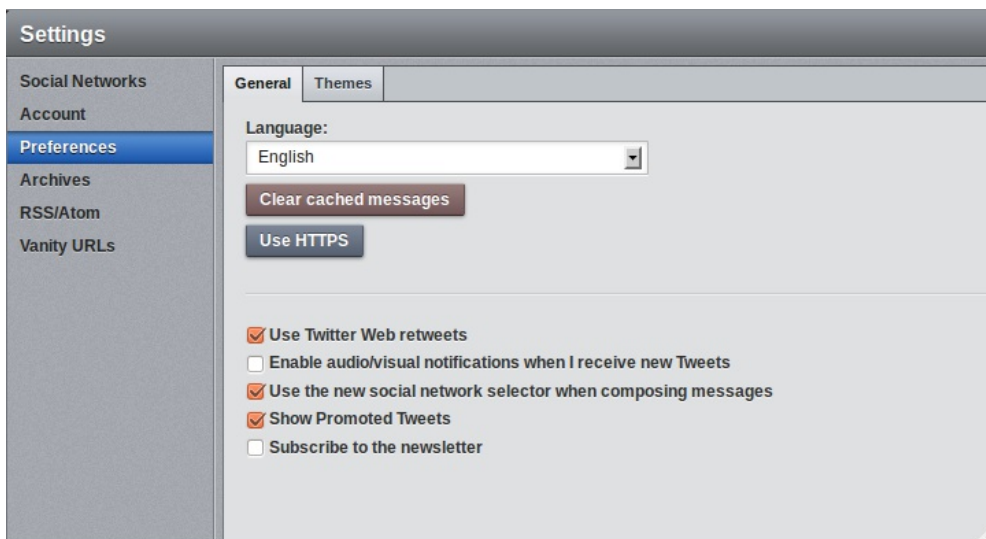
**HootSuite** est un **client Twitter** populaire qui permet aux utilisateurs de gérer et d'organiser un ou plusieurs comptes **Twitter** simultanément, de programmer des tweets, d'analyser des données liées aux interactions via **Twitter** et de faciliter l'utilisation collaborative de **Twitter** au sein d'organisations.

**Étape 1.** **HootSuite**, client **Twitter** par défaut, n'utilise pas de connexion chiffrée (**Secure Socket Layer**, aussi appelée **HTTPS**). Toutefois, il en propose l'option aux utilisateurs. **Cliquez** sur *Réglages* dans le menu à gauche, puis *Compte*.



Graphique 10 : Accueil HootSuite

**Étape 2.** Dans le menu Comptes, **cliquez** sur *Préférences*.



Graphique 11 : Préférences HootSuite.

Étape 3. Cliquez sur **Use HTTPS**.

## 2.4 Applications pour smartphones

Un certain nombre de clients et applications, y compris ceux mentionnés ci-dessus, sont également disponibles pour les smartphones tels que les iPhone, Androids, Blackberrys ou Windows Phones. Il est très important de garder à l'esprit que les smartphones présentent de certains problèmes de sécurité qui leur sont inhérents. L'utilisation de ces apps ou clients sur smartphones peut être moins sûre que sur votre ordinateur : il est possible par exemple qu'ils n'activent pas le cryptage SSL sur Twitter, exposant ainsi le contenu de vos tweets. Pour plus d'informations sur la façon de réduire les risques lors de l'utilisation de smartphones, consultez le [chapitre 11](#) <sup>[262]</sup>.

## Flickr

Fonctions : partage de photos/vidéos, partage de contenu Internet

**Flickr** appartient à Yahoo! et facilite également la connexion à partir d'autres comptes, y compris Google et Facebook.

Le contenu publié sur **Flickr** vous appartient. Vous pouvez y attribuer différentes licences Creative Commons ou droits d'auteur. En publiant, vous donnez à Yahoo! le droit de distribuer vos photos ou vidéos.

En raison de l'attribution diverse de licences, **Flickr** constitue une grande source d'images à utiliser pour des campagnes tout comme un outil pour partager des images avec des collègues, des amis ou des membres de vos réseaux.

Pour plus d'informations sur la protection des [données personnelles](#) <sup>[263]</sup>, consultez ces infographies sur le site [Me and My Shadow](#) <sup>[264]</sup>.

## Conseils sur Flickr

- Vérifiez que **Flickr** n'affiche pas d'informations cachées, enregistrées par votre appareil-photo numérique (métadonnées); ce qui peut inclure la date, l'heure, la localisation GPS, le type d'appareil-photo, etc.
- Ne jamais partager la photo d'une personne sur **Flickr** sans son consentement et soyez sûr que le sujet/s de chaque photo est d'accord avec le type de licence que vous avez choisi d'attribuer à leur image.

Le département de la Sécurité intérieure des États-Unis surveille **Flickr** et d'autres sites de réseautage social et il est fort probable que d'autres gouvernements en font de même.

## Alternatives à Flickr

Si vous ne souhaitez pas associer vos photos avec vos profils **Yahoo**, **Google** ou **Facebook**, il existe des alternatives. Des sites similaires sont peut-être plus populaires dans d'autres régions du globe et il se peut que vous souhaitiez explorer d'autres options. Avant de faire votre choix, tenez compte des points suivants :

1. Fournit-il une connexion via SSL pour toutes les utilisations du site plutôt que seulement durant la connexion ? Y-a-t-il des problèmes concernant le chiffrement tels que des problèmes liés aux certificats de chiffrement ?
2. Lisez attentivement le Contrat de Licence Utilisateur Final et la politique de confidentialité ou d'utilisation des données. Comment sont traités vos contenus et données ? Avec qui sont-ils partagés ?
3. Quelles options de confidentialité sont fournies aux utilisateurs ? Pouvez-vous choisir de partager vos vidéos en toute sécurité avec un petit nombre d'individus, ou bien sont-elles toutes publiques par défaut ?
4. Si vous téléchargez des images sensibles, tels des extraits de manifestations, le site facilite-t-il la protection de ceux que vous avez photographiés, notamment au moyen du floutage des visages ?
5. Connaissez-vous l'**emplacement géographique des serveurs**, la juridiction territoriale dont ils relèvent ou l'endroit où l'entreprise est inscrite ? Êtes-vous informé en quoi cette information concerne la confidentialité et la sécurité de votre usage de l'e-mail et de l'information ? Les propriétaires du site vont-ils transmettre des informations s'ils reçoivent une demande gouvernementale l'exigeant ?

# YouTube

## Short Description:

YouTube is a web service for video and other internet content sharing.

**YouTube** est idéal pour mettre vos vidéos à la disposition de ses milliards d'utilisateurs. Toutefois, comme **YouTube** appartient à **Google**, si les gens de **Google** trouvent le contenu de vos vidéos répréhensible, ils les supprimeront. Cela signifie que **YouTube** n'est pas un si bon endroit pour garder vos vidéos en sécurité. **Google** a également été appelé à céder à des pressions visant à supprimer du contenu de **YouTube** afin que le site ne soit pas censuré. Donc, si vous voulez que les gens voient votre vidéo, mettez-en une copie sur **YouTube** – mais pas l'unique copie. **YouTube** n'est pas un lieu de stockage sûr.

**Google** enregistrera les noms d'utilisateur et les données de localisation pour chaque vidéo téléchargée et visionnée. Cela peut être utilisé pour suivre et retrouver des individus.

Le contenu que vous publiez sur **YouTube** vous appartient ; en publiant sur **YouTube**, vous donnez toutefois le droit à **Google** de distribuer vos contenus.

**YouTube** est ou a été signalé comme inaccessible dans divers pays tels que : la Chine (depuis mars 2009), la Birmanie (entre mars 2010 et août 2011), l'Iran (depuis janvier 2011), la Libye (entre février et août 2011), la Syrie (depuis juin 2011) l'Ouzbékistan (depuis août 2011), la Tunisie, le Turkménistan, et la Turquie. Consultez le [Transparency Report section trafic de Google](#) [265] pour plus de détails.

Pour plus d'informations sur les [règles de confidentialité](#) [266] de **Google**, consultez ces infographiques sur le site [Me and My Shadow](#) [260].

## Conseils pour YouTube :

- Ne jamais publier une vidéo d'une personne sans son consentement. Et même avec son consentement, essayez de penser aux conséquences possibles avant de la publier.
- Lorsque vous allez sur **YouTube**, faites-le en tapant <https://www.youtube.com> dans la barre d'adresse de votre navigateur - la communication entre votre ordinateur et les serveurs de **YouTube** sera ainsi chiffrée par une connexion **Secure Socket Layer** (SSL). Pour éviter d'avoir à le faire à chaque fois que vous vous connectez, nous recommandons la connexion à **YouTube** via [Firefox](#) [247] avec des extensions telles que [HTTPS Everywhere](#) [267].
- Utilisez l'option **floutage des visages** de **YouTube** pour préserver l'anonymat de personnes dans des vidéos documentant par exemple des manifestations. Plus d'infos [ici](#) [268].
- Gardez toujours une copie de sauvegarde de chaque vidéo que vous partagez via Google/YouTube.
- Utilisez l'option Privée afin de partager vos vidéos avec des personnes bien précises.

## Alternatives à YouTube

Si vous ne souhaitez pas associer vos vidéos avec votre **profil Google**, il existe un certain nombre d'alternatives tel [Vimeo](#) [269]. Vimeo est fréquenté par une plus petite communauté d'utilisateurs que \*YouTube\*. Comme **YouTube**, il facilite la connexion via **SSL** et offre aux utilisateurs de nombreuses options de confidentialité et de contrôle sous licence Creative Commons pour leurs vidéos. D'autres sites similaires sont peut-être plus populaires dans d'autres régions du globe et vous souhaitez peut-être examiner d'autres options. Avant de faire votre choix, tenez compte des points suivants :

1. Fournit-il une connexion via SSL pour toutes les utilisations du site plutôt que seulement durant la connexion ? Y-a-t-il des problèmes concernant le chiffrement tels que des problèmes liés aux certificats de chiffrement ?
2. Lisez attentivement le Contrat de Licence Utilisateur Final et la politique de confidentialité ou d'utilisation des données. Comment sont traités vos contenus et données ? Avec qui sont-ils partagés ?
3. Quelles options de confidentialité sont fournies aux utilisateurs ? Pouvez-vous choisir de partager vos vidéos en toute sécurité avec un petit nombre d'individus, ou bien sont-elles toutes publiques par défaut ?
4. Si vous téléchargez des images sensibles, tels des extraits de manifestations, le site facilite-t-il la protection de ceux que vous avez filmés, notamment au moyen du floutage des visages ?
5. Connaissez-vous l'**emplacement géographique des serveurs**, la juridiction territoriale dont ils relèvent ou l'endroit où l'entreprise est inscrite ? Êtes-vous informé en quoi cette information concerne la confidentialité et la sécurité de votre usage de l'e-mail et de l'information ? Les propriétaires du site vont-ils transmettre des informations s'ils reçoivent une demande gouvernementale l'exigeant ?

---

URL source (Obtenu le 10/04/2014 - 10:33): <https://securityinbox.org/fr/handsonguides>

### Liens:

- [1] <https://securityinbox.org/fr/handsonguides>
- [2] <http://www.avast.com/fr-fr/free-antivirus-download>
- [3] <http://www.avast.com>
- [4] <https://securityinbox.org/fr/chapter-1>
- [5] <http://www.free-av.com/>
- [6] <http://free.avg.com/>
- [7] <http://www.avast.com/en-eu/mac-edition>
- [8] <http://www.kaspersky.co.uk/kaspersky-anti-virus-for-mac>
- [9] [http://www.mcafee.com/us/small/products/virussscan\\_for\\_mac/virussscan\\_for\\_mac.html](http://www.mcafee.com/us/small/products/virussscan_for_mac/virussscan_for_mac.html)
- [10] <http://www.sophos.com/products/enterprise/endpoint/security-and-control/>
- [11] <http://www.symantec.com/norton/products>
- [12] [https://securityinbox.org/fr/avast\\_virus#4.9](https://securityinbox.org/fr/avast_virus#4.9)
- [13] <https://securityinbox.org/sbox/programs/avast.exe>
- [14] <http://www.imgburn.com/>
- [15] <http://www.avg.com/us-en/avg-rescue-cd>
- [16] <http://support.kaspersky.com/viruses/rescuedisk/>
- [17] <http://www.f-secure.com/linux-weblog/files/f-secure-rescue-cd-release-3.00.zip>
- [18] [http://download.bitdefender.com/rescue\\_cd/](http://download.bitdefender.com/rescue_cd/)
- [19] <http://free.antivirus.com/hijackthis/>
- [20] <http://free.antivirus.com/clean-up-tools/>

[21] <http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx>  
[22] <http://technet.microsoft.com/en-us/sysinternals>  
[23] <http://www.avast.com/download-update>  
[24] <http://www.safer-networking.org/fr/mirrors/index.html>  
[25] <http://www.safer-networking.org/fr>  
[26] [https://securityinabox.org/fr/avast\\_principale](https://securityinabox.org/fr/avast_principale)  
[27] [https://securityinabox.org/fr/comodo\\_principale](https://securityinabox.org/fr/comodo_principale)  
[28] [https://securityinabox.org/fr/firefox\\_principale](https://securityinabox.org/fr/firefox_principale)  
[29] <http://superantispyware.com>  
[30] <http://www.malwarebytes.org/mbam.php>  
[31] <http://www.microsoft.com/windows/products/winfamily/defender>  
[32] <http://www.lavasoft.com/>  
[33] <http://www.javacoolsoftware.com/spywareblaster.html>  
[34] <https://securityinabox.org/sbox/programs/spybot.exe>  
[35] [https://securityinabox.org/spybot\\_advance](https://securityinabox.org/spybot_advance)  
[36] [https://security.ngoinabox.org/fr/ccleaner\\_registredewindows#4.0](https://security.ngoinabox.org/fr/ccleaner_registredewindows#4.0)  
[37] <https://securityinabox.org/fr/chapter-6>  
[38] <http://www.safer-networking.org/fr/howto/update.hs.html>  
[39] <http://personalfirewall.comodo.com/free-download.html>  
[40] <http://www.personalfirewall.comodo.com>  
[41] <http://www.netfilter.org/>  
[42] <https://help.ubuntu.com/community/Gufw>  
[43] <http://blog.bodhizazen.net/linux/firewall-ubuntu-gufw/>  
[44] <http://www.hanyynet.com/noobproof/>  
[45] <http://www.lobotomo.com/products/IPSecuritas/>  
[46] <http://www.obdev.at/products/littlesnitch/index.html>  
[47] <http://www.zonealarm.com/security/en-us/zonealarm-pc-security-free-firewall.htm>  
[48] <http://free.agnitum.com/>  
[49] [https://securityinabox.org/sbox/programs/cfw\\_installer.exe](https://securityinabox.org/sbox/programs/cfw_installer.exe)  
[50] <http://www.keepass.info/download.html>  
[51] [https://securityinabox.org/fr/keepass\\_utiliser](https://securityinabox.org/fr/keepass_utiliser)  
[52] <http://www.keepass.info/translations.html>  
[53] <http://www.keepass.info/>  
[54] <https://securityinabox.org/fr/chapter-3>  
[55] <http://www.keepassx.org/>  
[56] <http://passwordsafe.sourceforge.net/>  
[57] <http://agilewebsolutions.com/products/1Password>  
[58] <https://securityinabox.org/sbox/programs/KeePass-Setup.exe>  
[59] <https://securityinabox.org/sbox/programs/KeePass-fr.zip>  
[60] [https://securityinabox.org/fr/keepass\\_motsdepasse](https://securityinabox.org/fr/keepass_motsdepasse)  
[61] [https://securityinabox.org/fr/keepass\\_portable](https://securityinabox.org/fr/keepass_portable)  
[62] [http://security.ngoinabox.org/fr/recuva\\_principale](http://security.ngoinabox.org/fr/recuva_principale)  
[63] <http://www.truecrypt.org/downloads>  
[64] [https://securityinabox.org/fr/truecrypt\\_volumestandard#2.0](https://securityinabox.org/fr/truecrypt_volumestandard#2.0)  
[65] <http://www.truecrypt.org/localizations>  
[66] <http://www.truecrypt.org/>  
[67] <https://securityinabox.org/fr/chapter-4>  
[68] <http://www.ubuntu.com/>  
[69] <http://www.saout.de/misc/dm-crypt/>  
[70] <http://code.google.com/p/cryptsetup/>  
[71] <http://sd4l.sourceforge.net/>  
[72] <http://www.nathansheldon.com/files/>  
[73] [http://www.ce-infosys.com/english/free\\_compusec/free\\_compusec.aspx](http://www.ce-infosys.com/english/free_compusec/free_compusec.aspx)  
[74] <http://www.cryptooexpert.com/lite/>  
[75] <http://www.axantum.com/AxCrypt/>  
[76] <https://www.steganos.com/us/products/for-free/locknote/overview/>  
[77] <https://securityinabox.org/sbox/programs/TrueCrypt-Setup.exe>  
[78] <https://securityinabox.org/sbox/programs/TrueCrypt-fr.zip>  
[79] [http://security.ngoinabox.org/fr/truecrypt\\_portable](http://security.ngoinabox.org/fr/truecrypt_portable)  
[80] <http://www.truecrypt.org/docs/>  
[81] [https://securityinabox.org/fr/truecrypt\\_volumescaches](https://securityinabox.org/fr/truecrypt_volumescaches)  
[82] [https://securityinabox.org/fr/keepass\\_principale](https://securityinabox.org/fr/keepass_principale)  
[83] [https://securityinabox.org/fr/truecrypt\\_volumestandard#2.2](https://securityinabox.org/fr/truecrypt_volumestandard#2.2)  
[84] <http://forums.truecrypt.org/>  
[85] [http://security.ngoinabox.org/fr/truecrypt\\_principale](http://security.ngoinabox.org/fr/truecrypt_principale)  
[86] <http://www.truecrypt.org/faq.php>  
[87] <http://www.educ.umu.se/~cobian/cobianbackup.htm>  
[88] <https://securityinabox.org/sites/securitybkp.ngoinabox.org/security/files/cobian/Cb7Setup.exe>  
[89] <https://securityinabox.org/handsonguides>  
[90] <https://securityinabox.org/sites/securitybkp.ngoinabox.org/security/files/cobian/cbSetup8.exe>  
[91] <https://securityinabox.org/chapter-5>  
[92] <https://securityinabox.org/sbox/programs/cbSetup.exe>  
[93] [https://securityinabox.org/cobian\\_creer copie](https://securityinabox.org/cobian_creer copie)  
[94] <http://www.zipgenius.it/>  
[95] [https://securityinabox.org/cobian\\_chiffre](https://securityinabox.org/cobian_chiffre)  
[96] [https://securityinabox.org/truecrypt\\_principale](https://securityinabox.org/truecrypt_principale)  
[97] <https://securityinabox.org/chapter-4>  
[98] [https://securityinabox.org/cobian\\_compressor](https://securityinabox.org/cobian_compressor)  
[99] <http://www.piriform.com/recuva/builds>  
[100] <http://www.piriform.com/recuva>  
[101] <https://securityinabox.org/fr/chapter-5>  
[102] [http://www.r-tt.com/data\\_recovery\\_linux/](http://www.r-tt.com/data_recovery_linux/)  
[103] <http://www.cgsecurity.org/>  
[104] <http://ntfsundelete.com/>  
[105] <http://diskdigger.org/>  
[106] <http://www.pcinspector.de/Default.htm?language=1>  
[107] <http://undeleteplus.com/>  
[108] <https://securityinabox.org/sbox/programs/rcsetup.exe>  
[109] [https://securityinabox.org/fr/recuva\\_scan](https://securityinabox.org/fr/recuva_scan)  
[110] [https://securityinabox.org/fr/recuva\\_recuperer](https://securityinabox.org/fr/recuva_recuperer)  
[111] [https://securityinabox.org/fr/recuva\\_faq](https://securityinabox.org/fr/recuva_faq)  
[112] <http://www.heidi.ie>  
[113] <https://securityinabox.org/sites/securitybkp.ngoinabox.org/security/files/eraser/EraserSetup32.exe>  
[114] <https://securityinabox.org/chapter-6>  
[115] <https://securityinabox.org/sbox/programs/EraserSetup32.exe>  
[116] [https://securityinabox.org/undelete\\_principale](https://securityinabox.org/undelete_principale)  
[117] [https://securityinabox.org/ccleaner\\_principale](https://securityinabox.org/ccleaner_principale)  
[118] <http://www.piriform.com/ccleaner/builds>  
[119] <http://www.ccleaner.com>  
[120] <http://bleachbit.sourceforge.net/>  
[121] [http://doc.ubuntu-fr.org/nettoyer\\_ubuntu](http://doc.ubuntu-fr.org/nettoyer_ubuntu)  
[122] <http://www.titanium.free.fr/>

[123] <https://securityinabox.org/sbox/programs/ccsetup.exe>  
[124] [https://securityinabox.org/fr/ccleaner\\_questions](https://securityinabox.org/fr/ccleaner_questions)  
[125] <https://riseup.net/>  
[126] <https://securityinabox.org/fr/chapter-7>  
[127] [http://security.ngoinabox.org/fr/thunderbird\\_principale](http://security.ngoinabox.org/fr/thunderbird_principale)  
[128] [https://securityinabox.org/fr/riseup\\_modifieparametres#4.3](https://securityinabox.org/fr/riseup_modifieparametres#4.3)  
[129] <https://mail.riseup.net>  
[130] <https://help.riseup.net/security>  
[131] <https://mail.riseup.net/>  
[132] <https://user.riseup.net/>  
[133] [https://securityinabox.org/riseup\\_creeruncompte#2.1](https://securityinabox.org/riseup_creeruncompte#2.1)  
[134] <http://www.pidgin.im/download/windows/>  
[135] <http://www.cypherpunks.ca/otr/index.php#downloads>  
[136] <http://www.pidgin.im>  
[137] <http://www.cypherpunks.ca/otr/>  
[138] <http://www.miranda-im.org/>  
[139] <http://adium.im/>  
[140] <http://dashboard.aim.com/aim>  
[141] <http://www.apple.com/support/bonjour/>  
[142] <http://komunikator.gadu-gadu.pl/>  
[143] <http://www.google.com/talk/>  
[144] <http://www.icq.com>  
[145] <http://www.mirc.com/>  
[146] <http://www.msn.com/>  
[147] <http://www.mxit.com/>  
[148] <http://www.myspace.com/guide/im>  
[149] <http://www.qq.com/>  
[150] <http://silcnet.org/>  
[151] <http://www.ibm.com/developerworks/downloads/ls/lst/>  
[152] <http://messenger.yahoo.com/>  
[153] <https://securityinabox.org/sbox/programs/pidgin.exe>  
[154] <https://securityinabox.org/sbox/programs/pidgin-otr.exe>  
[155] [https://securityinabox.org/fr/pidgin\\_googletalk](https://securityinabox.org/fr/pidgin_googletalk)  
[156] <mailto:thierry.letesteur@gmail.com>  
[157] [https://securityinabox.org/fr/pidgin\\_googletalk#5.1](https://securityinabox.org/fr/pidgin_googletalk#5.1)  
[158] <http://www.google.com>  
[159] [https://securityinabox.org/fr/pidgin\\_utiliser#2.4](https://securityinabox.org/fr/pidgin_utiliser#2.4)  
[160] <https://www.vaultletsoft.com/>  
[161] <http://www.vaultletsoft.com/start/downloads.html>  
[162] <https://securityinabox.org/chapter-7>  
[163] [https://securityinabox.org/sbox/programs/VaultletSuite2Go\\_windows.exe](https://securityinabox.org/sbox/programs/VaultletSuite2Go_windows.exe)  
[164] <mailto:terrence.letesteur@vaultletsoft.com>  
[165] [https://securityinabox.org/vaultletsuite\\_questions](https://securityinabox.org/vaultletsuite_questions)  
[166] <http://www.mozillamessaging.com/fr/thunderbird/>  
[167] <http://enigmail.mozdev.org/download/index.php>  
[168] <http://www.gnupg.org/download/index.en.html#auto-ref-2>  
[169] <http://www.mozilla.com/thunderbird/>  
[170] <http://enigmail.mozdev.org/home/index.php>  
[171] <http://www.gnupg.org/>  
[172] <http://www.claws-mail.org/>  
[173] <http://sylpheed.sraoss.jp/en/>  
[174] <http://www.washington.edu/alpine/>  
[175] <https://www.google.com/accounts/NewAccount?service=mail>  
[176] [http://security.ngoinabox.org/en/riseup\\_createaccount](http://security.ngoinabox.org/en/riseup_createaccount)  
[177] <https://securityinabox.org/sbox/programs/Thunderbird-fr.exe>  
[178] <https://securityinabox.org/sbox/programs/enigmail.xpi>  
[179] <https://securityinabox.org/sbox/programs/gnupg-w32cli-1.4.9.exe>  
[180] <http://security.ngoinabox.org/en/node/1451#3.3>  
[181] [https://securityinabox.org/fr/thunderbird\\_securite](https://securityinabox.org/fr/thunderbird_securite)  
[182] [https://securityinabox.org/avast\\_principale](https://securityinabox.org/avast_principale)  
[183] [https://securityinabox.org/comodo\\_principale](https://securityinabox.org/comodo_principale)  
[184] [https://securityinabox.org/spybot\\_principale](https://securityinabox.org/spybot_principale)  
[185] [https://securityinabox.org/fr/firefox\\_autres](https://securityinabox.org/fr/firefox_autres)  
[186] [https://securityinabox.org/fr/thunderbird\\_utiliserenigmail](https://securityinabox.org/fr/thunderbird_utiliserenigmail)  
[187] [http://fr.wikipedia.org/wiki/Cryptographie\\_asym%C3%A9trique](http://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique)  
[188] <http://www.mozilla.org/fr/firefox/fix/>  
[189] <https://addons.mozilla.org/en-US/firefox/addon/noscript/>  
[190] <https://addons.mozilla.org/en-us/firefox/addon/adblock-plus/>  
[191] <https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/>  
[192] <https://addons.mozilla.org/en-US/firefox/addon/beef-taco-targeted-advertising/>  
[193] <https://addons.mozilla.org/en-US/firefox/addon/googlesharing/>  
[194] <https://www.eff.org/https-everywhere>  
[195] <http://www.google.com/chrome/>  
[196] <http://www.opera.com/>  
[197] [https://securityinabox.org/fr/firefox\\_noscript](https://securityinabox.org/fr/firefox_noscript)  
[198] <http://www.virustotal.com/>  
[199] <http://onlinelinkscan.com/>  
[200] <http://www.phishtank.com/index.php>  
[201] <http://safeweb.norton.com/>  
[202] <http://www.urlvoid.com/>  
[203] <https://securityinabox.org/sbox/programs/Firefox-fr.exe>  
[204] <https://securityinabox.org/sbox/programs/noscript.xpi>  
[205] <https://securityinabox.org/sbox/programs/adblock-plus.xpi>  
[206] <https://securityinabox.org/sbox/programs/better-privacy.xpi>  
[207] <https://securityinabox.org/sbox/programs/beef-taco.xpi>  
[208] <https://securityinabox.org/sbox/programs/googlesharing.xpi>  
[209] <https://securityinabox.org/sbox/programs/https-everywhere.xpi>  
[210] [https://securityinabox.org/fr/firefox\\_portable](https://securityinabox.org/fr/firefox_portable)  
[211] [https://securityinabox.org/fr/ccleaner\\_principale](https://securityinabox.org/fr/ccleaner_principale)  
[212] <https://addons.mozilla.org/fr/firefox/>  
[213] <https://www.mozilla.com/fr/plugincheck>  
[214] <https://www.torproject.org/easy-download.html.fr>  
[215] <https://www.torproject.org/>  
[216] <https://securityinabox.org/fr/node/337>  
[217] <http://hotspotshield.com/>  
[218] <http://www.dit-inc.us/freegate>  
[219] <http://www.ultrareach.com/>  
[220] <http://www.your-freedom.net/>  
[221] <http://psiphon.ca/>  
[222] <http://sesawe.net/>  
[223] <https://securityinabox.org/sbox/programs/tor-browser-fr.exe>  
[224] <https://securityinabox.org/fr/node/701>

[225] <https://securityinabox.org/fr/node/784>  
[226] <https://check.torproject.org/>  
[227] [https://securityinabox.org/fr/tor\\_problemes](https://securityinabox.org/fr/tor_problemes)  
[228] <http://www.dailymotion.com/>  
[229] <http://hub.witness.org/>  
[230] <http://www.youtube.com>  
[231] <https://www.torproject.org/torbutton/>  
[232] <https://www.torproject.org/torbutton/torbutton-faq.html.en>  
[233] <https://wiki.torproject.org/noreply/TheOnionRouter/TorFAQ>  
[234] <https://mail.google.com>  
[235] <https://bridges.torproject.org/>  
[236] [https://securityinabox.org/fr/tor\\_reseau](https://securityinabox.org/fr/tor_reseau)  
[237] <https://securityinabox.org/fr/chapter-8>  
[238] <https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/TorFAQ>  
[239] <https://securityinabox.org/fr/node/1945>  
[240] <http://joindiaspora.com>  
[241] <http://we.riseup.net>  
[242] <http://friendica.com/>  
[243] <https://pidder.com>  
[244] <http://secushare.org>  
[245] <http://socialswarm.net>  
[246] <http://www.facebook.com>  
[247] [https://securityinabox.org/en/firefox\\_main](https://securityinabox.org/en/firefox_main)  
[248] [https://securityinabox.org/en/tor\\_main](https://securityinabox.org/en/tor_main)  
[249] <https://securityinabox.org/fr/fr/node/1945>  
[250] <https://www.facebook.com/legal/terms>  
[251] <https://www.facebook.com/about/privacy/>  
[252] <http://www.facebook.com/about/privacy>  
[253] <https://www.myshadow.org/content/facebook-info-we-receive>  
[254] <https://www.twitter.com>  
[255] <https://securityinabox.org/chapter-10>  
[256] <https://www.twitter.com/tos>  
[257] <https://www.twitter.com/privacy/>  
[258] [https://securityinabox.org/fr/chapter\\_7\\_1](https://securityinabox.org/fr/chapter_7_1)  
[259] <http://twitter.com/privacy>  
[260] <https://www.myshadow.org/lost-in-small-print>  
[261] <http://www.mozilla.org/en-US/dnt/>  
[262] <https://securityinabox.org/en/chapter-11>  
[263] <http://info.yahoo.com/privacy/fr/yahoo/>  
[264] <https://www.myshadow.org/content/yahoo-collection>  
[265] <https://www.google.com/transparencyreport/traffic/?hl=fr>  
[266] <http://www.google.com/intl/fr/policies/privacy/>  
[267] [https://securityinabox.org/en/firefox\\_others#5.5](https://securityinabox.org/en/firefox_others#5.5)  
[268] <http://support.google.com/youtube/bin/static.py?hl=fr&guide=1388381&hlrm=en&page=guide.cs&answer=2640535>  
[269] <https://www.vimeo.com>